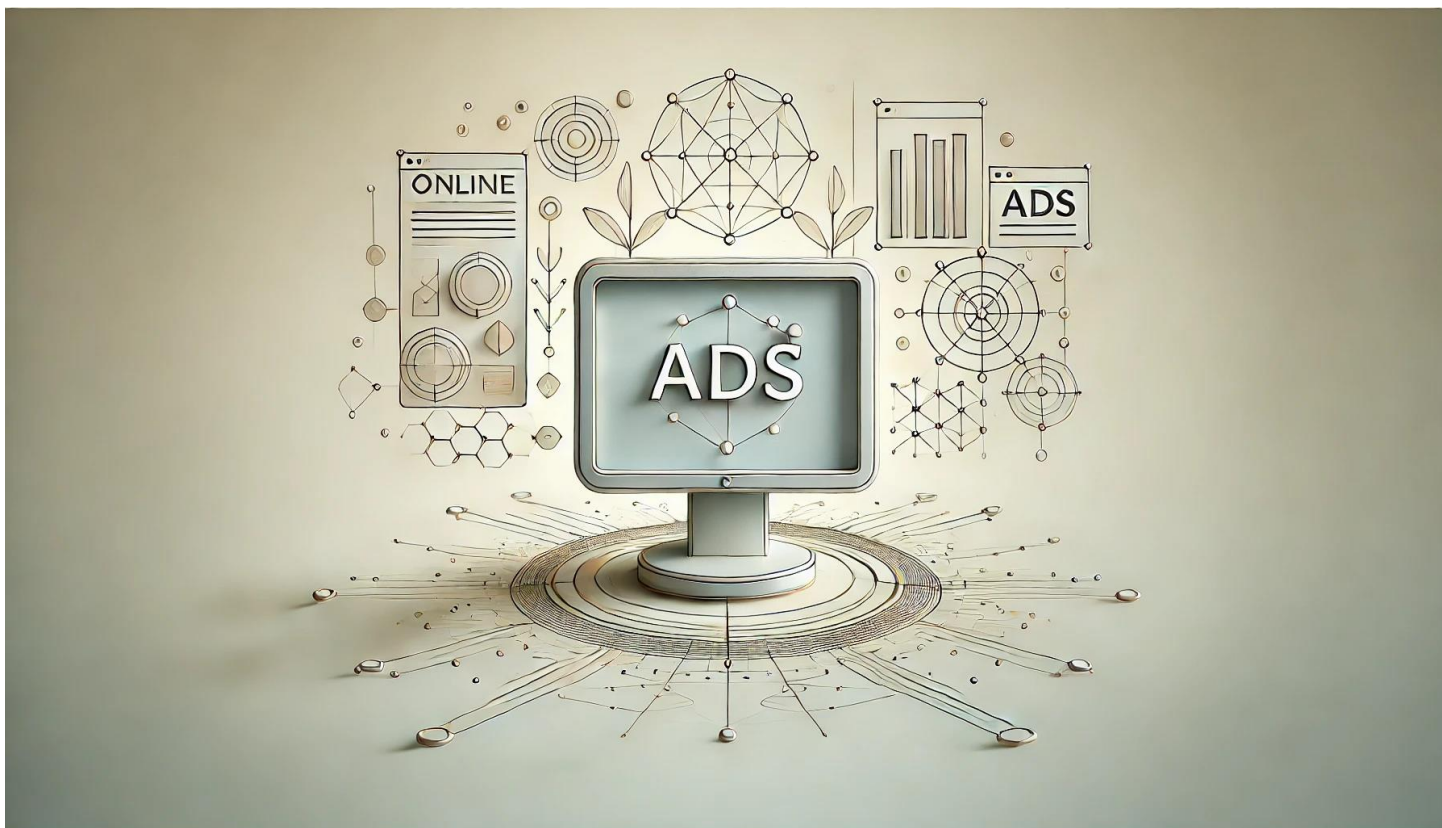




Final Report

Online Behavioral Advertising Microtargeting, data & consumer protection issues

This research project is supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the Action called “2nd Call for Research Projects by H.F.R.I. for the support of Faculty Members and Researchers” [Project “Online Behavioral Advertising: Microtargeting, data and consumer protection issues” (O.B.A.M.A.) Project No. 4246]

Preface

The research project "Online Behavioral Advertising and Microtargeting Activities" (OBAMA - 4246 - the "Project"), funded by the Hellenic Foundation for Research & Innovation (HFRI) under the "2nd Call for Research Projects by HFRI to support University Faculty Members and Researchers," set out three primary objectives:

(a) To identify the key regulatory and legal issues concerning data protection in the context of Online Behavioral Advertising (from now on referred to as "OBA"), highlighting the interpretative challenges and gaps in the legal framework, as well as the interaction between the impact of unlawful data processing and consumer protection.

(b) To assess the level of understanding, on the one hand of users regarding the functioning of Online Behavioral Advertising (OBA) and their rights both as data subjects and consumers and, on the other hand, of businesses operating online about their corresponding obligations.

(c) To utilize the findings of the research on the legal framework and the perceptions of users and businesses regarding OBA to provide useful information to legislators, competent authorities, businesses, and internet users.

The final deliverable of the Project is this Report, which constitutes the first comprehensive review of OBA through the lens of data protection and consumer protection legislative systems in Greece. The Report consists of three parts:

A. The first part presents the legal framework concerning OBA from the perspective of data protection laws as well as privacy and consumer rights, analyzing specific parameters identified by the research team as the most critical, such as the legal basis for data processing and the use of technologies for tracking users' online behavior, transparency, consumer behavior distortion, and the conditions for making informed transactional decisions by consumers without undue external influence. The first part aims to provide an up-to-date, complete, and accurate overview of the legal framework concerning OBA,

recording and assessing significant developments that took place during the research project. Additionally, the specific issues arising from OBA concerning the legal framework for processing personal - and non-personal - data, as well as consumer protection, are examined.

B. The second part focuses on the perceptions of users and businesses regarding OBA, particularly as reflected in the surveys conducted as part of the research project. The objective of the second part is to evaluate the legal research findings, in light of the information provided through questionnaires to consumers and professionals, concerning the awareness and understanding of users about their rights, as well as the obligations of businesses regarding OBA.

C. The third part includes both the evaluation of the findings from the previous stages of the research (analysis of the legal framework and perceptions of its practical application) and guidelines for the involved parties aiming at more effective protection of users/consumers. Starting from identifying areas that raise concerns regarding the de facto compliance with legislation in online practice, combined with the expectations and objectives of consumers and businesses, the research team developed guidelines addressed to three distinct groups with corresponding goals:

(a) To internet users, aiming to raise their awareness of issues concerning online advertising and particularly the so-called microtargeting¹. It is the team's firm belief, based on the research findings, that a well-informed user can more effectively understand and assert their rights both as a data subject and as a consumer.

¹ Microtargeting is a practice that uses consumer data and demographic information to determine the interests of specific individuals, particularly in the field of political advertising. See related: "MEPs vote for tougher rules on political advertising" available at https://www.europarl.europa.eu/pdfs/news/expert/2023/2/press_release/20230130IPR70208/20230130IPR70208_en.pdf

(b) To businesses, aiming to inform them about the operation and legality of the online advertising and microtargeting practices they adopt. The goal is to clarify these practices' potential legal risks, considering data protection, privacy, and consumer protection laws.

(c) To the competent authorities overseeing data protection and ensuring consumer protection. Based on a comprehensive and up-to-date legal analysis of the issues, the Report offers recommendations on effectively carrying out their duties and taking legislative or regulatory initiatives in specific areas identified during the research.

We hope our research will contribute to the national, EU, and international dialogue on regulating online advertising and serve as a catalyst for raising awareness of these issues among all stakeholders in Greece.

The Research Team:

Evangelia (Lilian) Mitrou, Professor at the Department of Information and Communication Systems Engineering, University of the Aegean

Michail Avgoustianakis, Professor of Civil Law at the Law School of the National and Kapodistrian University of Athens

Dimitris Drosos, Assistant Professor at the Department of Marketing and Communication, Athens University of Economics and Business

Evangelos Margaritis, Lawyer, Dr. of Law, Postdoctoral Researcher (PostDoc) in Civil Law at the Athens Law School

Vassilis Karkatzounis, PhD Candidate at the Department of Information and Communication Systems Engineering, University of the Aegean

Elpida Efstathiou, PhD Candidate at the Department of Marketing and Communication, Athens University of Economics and Business

Introduction

1. A brief overview of Online Advertising

Online advertising is one of the most complex and intriguing issues, viewed through the lens of the Internet economy and the protection of user autonomy and privacy. Although advertising has been an integral part of the online environment since its early days, in recent years - as a core funding model for online businesses - it has become associated with and characterizes every aspect of internet browsing. According to IAB Europe², the value of digital advertising expenditure in Europe alone reached almost €97 billion in 2023, reflecting an increase of €36 billion compared to 2020.³

The vast amount of available digital data and enhanced, low-cost computing power created ideal conditions for adopting intrusive advertising methods while disrupting traditional business models, fundamentally affecting the interaction between businesses and consumers. The increasing use and effectiveness of advertising technologies, commonly referred to as "Adtech" (Advertising Technologies), in data analysis and transaction automation have contributed to online advertising quickly surpassing traditional forms of advertising and gradually establishing a new status quo.⁴ Online advertising relies heavily on the extensive use of "cookies"⁵ and similar technologies (web beacons, pixels),

² The Interactive Advertising Bureau - IAB is an organization of advertising businesses that develops industry standards, conducts research, and provides legal support in the field of online advertising. The organization represents many of the most well-known media outlets worldwide, but primarily in the United States, Canada, and Europe.

³ AdEx Benchmark 2023 Report, available at https://iabeurope.eu/wp-content/uploads/IAB-Europe_AdEx-Benchmark-2023-Report.pdf

⁴ Giovanni Sartor, "New aspects and challenges in consumer protection: Digital services and artificial intelligence" (2020), Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament

⁵ **Cookies** are small text files installed on users' terminal devices (computer, tablet, mobile device) with a wide range of functions, from remembering each user's preferences (e.g., username and passwords) or

collectively known as trackers⁶. Tracking a user's online behavior covers various aspects, such as the websites they visit, the duration of their stay/browsing, the content viewed, the ads they interact with, and more. Tracking, combined with data that users have voluntarily disclosed (e.g., gender, age, residence, nationality), forms the cornerstone of the modern advertising ecosystem, enabling the creation of user profiles based on a range of criteria through the extensive processing of personal data. However, this intrusive and increasingly pervasive use of trackers raises several issues regarding the application of the General Data Protection Regulation (GDPR)⁷, making data processing for advertising purposes one of the most debated topics in internet and new technologies law.

2. Types of Online Advertising

Targeted advertising is a commercial practice that utilizes data, often of a personal nature, relating to specific characteristics of individuals or their online behavior and habits, aiming to select and display the most relevant advertisements to them. According to the European Commission⁸, targeted advertising is a category that includes:

Contextual Advertising “targets” users based on the website content they are visiting or the keyword they have entered into a search engine.

website appearance settings to measuring visits to a website or tracking user activity for the purpose of creating their advertising profile.

⁶ Hellenic Data Protection Authority, Recommendations for the compliance of data controllers with specific legislation on e communications, available at <https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythnon-epexedomenon-me-tin-eidiki>

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

⁸ European Commission (2018), Consumer market study on online market segmentation through personalised pricing/offers in the European Union, Final Report, available at https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through-personalised-pricing-offers-european-union_en

Segmented Advertising, delivered according to user characteristics (such as age, gender, profession, location), is typically provided by the users, e.g., during website registration.

Behavioral Advertising (OBA) is based on observing users' online behavior over time and processing data that they have disclosed or that is generated or inferred about them. OBA is a targeted advertising method that follows users' preferences, choices, or interests to present relevant ads and includes various sub-methods, such as retargeting.⁹

The significant commercial advantage of OBA is its ability to display advertisements relevant to each user's preferences, thereby minimizing unnecessary advertising campaigns. Ads "tailored" to each user appear to have greater acceptance among users, making OBA much more effective than other types of advertising. This can also have positive outcomes for internet users, as the suggested ads are likely to align with their preferences and facilitate the purchase of products and services that are more useful to them.¹⁰

OBA is at the core of the business model and constitutes the primary revenue source for major social media platforms, such as Facebook, TikTok, and Instagram, as well as intermediary service providers like Google and Amazon. These tech giants have developed economic models based on providing free access and use of their services. The flip side of this model is generating revenue from advertisements based on personal data, which serve as a de facto exchange for accessing services. The extraction, evaluation, and further data processing and utilization ultimately drive these companies' enormous profits.¹¹

⁹ Retargeting focuses on displaying targeted ads to recapture the attention of potential customers based on their previous online behavior.

¹⁰ J Zuiderveen Borgesius, Improving privacy protection in the area of behavioral targeting (Wolters Kluwer 2015)

¹¹ The Commodification of the Individual in the Internet Era: Informational Self-determination or "Selfalienation"? p. 475, Proceedings of the 8th International Conference Computer Ethics: Philosophical Enquiry. Also see I van Ooijen, H U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) Journal of Consumer Policy 91–107

It should be noted that these platforms not only use user data to deliver ads on their respective websites but have also created massive advertising networks that hold the largest share in the relevant sector¹². By utilizing advanced analytics tools, platforms enable advertisers to monitor how consumers interact with displayed ads and then, based on the performance of these ads, optimize their practices to target the "right" recipients even more effectively. In this context, the so-called "ad exchanges" thrive—intermediary online platforms where ad space can be bought and sold (even in real-time) based on bid submissions within predefined supply and demand parameters¹³.

3. Risks Arising from OBA

At this point, we encounter the darker "threat" posed by the use of Online Behavioral Advertising (OBA) to users' rights, both as data subjects¹⁴ and as consumers¹⁵. Behavioral targeting of internet users can pose significant risks, not only to their privacy in a narrow sense but also to their personal autonomy in a broader sense. Users cannot be sure about the circulation of their data in the online environment, the processing it undergoes, or the uses to which it may be put. Individuals are likely unaware or have minimal knowledge of the conditions under which their personal data is collected, sold, or transferred. Large volumes of data generated through tracking techniques are processed by intermediaries in

¹² See for example the UK Competition and Markets Authority's Investigation into suspected anti-competitive conduct by Google in ad tech, available at <https://www.gov.uk/cma-cases/investigation-into-suspected-anti-competitive-conduct-by-google-in-ad-tech>

¹³ Giovanni Sartor κ.ά., Regulating targeted and behavioural advertising in digital services

¹⁴ According to Article 4 of the GDPR, "personal data" refers to any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

¹⁵ According to Article 1a of Law 2251/1994, a consumer is defined as any natural person who acts for purposes that do not fall within their commercial, business, craft, or professional activity.

the AdTech value chain, often without sufficient safeguards to ensure that the principles and rules of data processing, as enshrined and enforced by the General Data Protection Regulation (GDPR), are adhered to.

Modern data analytics tools allow for the recognition of each user's mindset, perceptions, beliefs, and opinions with great accuracy. AdTech intermediaries can discern users' needs, cognitive biases, fears, and vulnerabilities, exploiting these to offer personalized content.¹⁶ This reality creates a new form of "transactional exploitation," blurring the lines between legitimate or standard marketing techniques and the unfair deception or manipulation of users' choices or even outright deceit.

In a digital environment, each user's footprint can be collected, analyzed, categorized, and ultimately used to manipulate and shape their choices. One might describe this as "digital nudging." This practice can push users toward an unconscious, predetermined choice directed by the party that paid the most for displaying the personalized advertisement. Thus, Advertising shifts from a medium for promoting products and services to a model for bypassing users' decision-making ability¹⁷. Data processing within the framework of OBA makes data subjects vulnerable to influence and manipulation, as targeted advertising and news shape their online experience, exploiting their attention and directing their actions toward goals and in ways that may not serve the users' interests. The legal boundaries for the lawful use of OBA as a market practice remain unclear, as the next section will show.

Today, OBA is the dominant form of advertising and a primary revenue source for a wide range of services. An entire business model has developed around online advertising, providing access to online services and content without monetary compensation—or, more

¹⁶ Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019

¹⁷ F J Zuiderveen Borgesius, N Helberger, A Reyna, 'The perfect match? a closer look at the relationship between EU consumer law and data protection law' (2017) 54(5) Common Market Law Review, 1427 - 1465

pragmatically, models where user data and attention¹⁸ serve as compensation in exchange for access to a platform¹⁹.

However, beyond the economic significance of online advertising, the entrenched adoption of behavioral microtargeting practices within the OBA framework has long-term implications for users, not only as data subjects and consumers but also as citizens of a democratic society. On the modern internet, detailed user profiles are developed through processes based on opaque algorithmic procedures, with minimal or no human intervention. The risks arising from the creation of these profiles are multi-faceted, as they are closely linked to the core of human autonomy. Simply put, the more we know about a person, the easier it is to control them. The microtargeting model ultimately shapes not just consumer consciousness, but also social and cognitive consciousness, reaching into the very core of human thought. This issue has prompted the present research.

¹⁸ Trzaskowski, Jan, Your Privacy Is Important to Us! – Restoring Human Dignity in Data-Driven Marketing (December 6, 2021). Copenhagen Business School, CBS LAW Research Paper No. 21 -10, Ex Tuto Publishing

¹⁹ Galli, Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD. in Ebers, M., Cantero Gamito, M. (eds) Algorithmic Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law, vol 1. Springer (2021), 110

Part One:

The Legal Framework for OBA

1. Introduction

OBA is one of the most popular, advanced, and simultaneously controversial methods of online advertising, based on extensive collection and analysis of user data. This form of advertising exploits information such as user preferences as reflected in their internet browsing, their searches, their activity on social media, and a plethora of personal data, such as age, gender, etc., in order to display targeted advertisements that respond to the interests and needs of each user. Despite its benefits, such as optimizing advertising performance and offering personalized experiences, the use of OBA justifiably raises severe concerns regarding protecting users' privacy and personal data, as well as consumer protection.

The risks of OBA are varied and multi-layered. Initially, the unprecedented data collection and analysis can lead to a violation of users' private sphere, creating a detailed profile without meeting the required conditions of the legal framework. The issue of the legality of data processing is of particular interest and was at the center of the Project's research, as it is linked to both legal parameters and market and technology issues, such as how user consent is obtained and user experience. As will be analyzed further, within a complex technological environment where users are constantly and daily faced with consent requests to which they often respond uncritically, consent as a tool for ensuring the informational self-determination of the individual is being tested and placed under intense scrutiny.

A major issue is also the lack of transparency in data collection practices and inadequate information to users about the use of their data. The information asymmetry is particularly evident in the OBA environment, where advertising companies, online platforms, and social media collect vast amounts of data and form detailed profiles of users, who have little or

no knowledge of the terms of collection and processing of their data. This inequality, in conjunction with other widespread practices in online advertising, such as retargeting, dark patterns²⁰, need creation, and aggressive commercial practices, undermines users' ability to make informed decisions, both as data subjects and as consumers, and can often lead, quite justifiably, to feelings of exploitation and suspicion.²¹

At the same time, the over-concentration of data on user behavior and preferences by tech giants poses significant risks to competition and the smooth functioning of the market.²² The situation is made even more complex by the tendency of these companies to use data protection concerns as a pretext to further strengthen their market position, a practice particularly prevalent in the online advertising space in recent years.

Regarding OBA and its utilization, another significant aspect is identified concerning consumer protection and touching on the corresponding law. OBA is conducted for the purpose of financing websites, platforms, and applications. However, many other parties participate in the value chain of online advertising as intermediaries in the display of advertising messages related to products or services of third-party advertisers. The purpose of advertising is to shape consumer consciousness, targeting (literally and metaphorically) elements even at the core of the private sphere of internet users, which they know by monitoring their behavior, inferring these from observing user patterns on the internet, or even guessing them based on advanced analytical algorithmic tools. Consequently, OBA constitutes a "commercial practice". As a commercial practice, to the extent that it

²⁰ Jarovsky, Luiza, Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness, EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them

²¹ A Jabłonowska, 'Consumer Protection in the Age of Data-Driven Behaviour Modification' (2022) EuCML, 67, 69.

²² Geradin, Damien and Katsifis, Dimitrios and Karanikioti, Theano, GDPR Myopia: How a WellIntended Regulation ended up Favoring Google in Ad Tech (May 11, 2020). TILEC Discussion Paper No. 2020-012

addresses consumers, it falls under consumer protection legislation (Law 2251/1994, as will be analyzed below) and is evaluated based on this, as well.

Finally, OBA carries severe risks of discriminatory treatment of individuals or groups of individuals based on specific characteristics such as their health status, sexual preferences, or political views²³. At the same time, OBA is associated with broader, collective risks at the market level, such as the over-concentration of data in an oligopoly, as well as societal risks, such as the spread of illegal content and misinformation. However, OBA methods are also extensively utilized in the context of political advertising. Consequently, manipulation and targeting of vulnerable groups that influence their decisions in an opaque and irrational way can pose significant risks even to the integrity of elections and other democratic processes.

2. Legislation related to OBA

Before the start of the research project, several pieces of legislation were already in force at the European Union level that contained provisions regarding online advertising. Other legislative initiatives in the EU were completed during the research project, such as the Digital Services Act and the Digital Markets Act, which set new rules and "target" OBA and large platforms. In order to form a comprehensive picture of the legal framework for online advertising, a presentation and brief analysis of the legislation for online advertising follows. The extent of the analysis varies based on the degree of impact of each piece of legislation on the regulatory environment of online advertising.

2.1. General Data Protection Regulation (Regulation 2016/679)

The General Data Protection Regulation (GDPR) applies to the processing of personal data, primarily aiming to regulate (fully or partially) automated processing. Both the concept of

²³ Wachter, Sandra, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising (May 15, 2019). Berkeley Technology Law Journal, Vol. 35, No. 2, 2020

processing and personal data, as defined in Article 4 GDPR, have been broadly interpreted by the EU Court of Justice²⁴ and include a wide range of functions related to OBA, including profiling and trackers used²⁵. The GDPR is one of the most fundamental pieces of legislation for regulating online advertising, establishing strict regulations both in the context of the relationship between the data controller and the data subject (end-user) and between the participants in the online advertising ecosystem (either as data controllers or processors).

The GDPR explicitly includes two references to cookies, which are currently the primary technological means for OBA, as well as online advertising in general, and other identifiers. Recital 30 of the Regulation notes that “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, particularly when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them”. Additionally, Recital 58 states that “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. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is particularly relevant in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to them are being collected, such as in the case of online advertising. Given that children merit specific protection, any

²⁴ See, for example, the decisions of the Court of Justice of the EU in Pankki S, C-579/21, Planet49, C-673/17, and IAB Europe, C-604/22.

²⁵ See, for example, the decision of the Court of Justice of the EU in IAB Europe, C-604/22, where it was ruled that even a string consisting of a combination of letters and characters, such as the TC String (Transparency and Consent String), which contains a user's preferences regarding consent, constitutes personal data.

information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand." Therefore, the GDPR explicitly links OBA with the use of technologies that allow user tracking and the lack of transparency in the complex and crowded online advertising ecosystem²⁶.

The individual data processing acts in the context and for the purposes of OBA should be carried out in compliance with the principles included in Article 5 of the GDPR, such as purpose limitation and data minimization, while Data Controllers should be able to demonstrate their compliance with the relevant rules (principle of accountability). The GDPR requires Data Controllers to provide clear and understandable information about data collection and processing, as well as to respect the rights of data subjects, such as the right of access (Article 15), rectification (Article 16), and erasure (Article 17) of their data.

The principle of minimization, according to Article 5 GDPR, requires processing only the essential personal data for each specific purpose, which in this case is the display of targeted advertisements, and should be known to the data subject in advance. In the case of OBA, this implies the collection and processing of only the data necessary for providing targeted advertisements, a parameter that is difficult to satisfy in the context of advertising systems that exhibit data bulimia. Similarly, the application of the principle of data security in online advertising presents significant challenges, as in modern OBA systems, technical and organizational measures are often inadequate in view of the increased individual and social risks.

A characteristic example is Google's Real Time Bidding (RTB) system, an impressively fast and widely used programmatic advertising application²⁷. RTB involves a vast number of interested parties, such as advertising networks and data management platforms, which

26 Article 29 Working Party Opinion 2/2010 on Online Behavioral Advertising

²⁷ <https://developers.google.com/authorized-buyers/rtb/start>

collaborate in complex and often opaque systems, allowing advertisers to offer targeted advertisements. In simple terms, when a user visits a website, ad auctions occur in the background, during which personal information about the user's characteristics, behavior, and preferences is exchanged between interested parties to find the ideal recipient for each advertisement²⁸. This massive-scale data processing has raised serious concerns about the adequacy of security measures from the design stage as well as accountability mechanisms, leading to the characterization of the system as the "biggest data breach in history."²⁹

Based on the principle of lawfulness, data processing must also be grounded in one of the legal bases provided in Article 6 of the GDPR. In the context of online advertising, only three out of the six available legal bases could be applicable, specifically consent, legitimate interest, and contract. According to the prevailing opinion in theory and jurisprudence, the data subject's consent is the predominant, if not the sole, processing basis for OBA. However, meeting the strict requirements set by the GDPR for providing lawful consent in the case of online advertising is a particularly challenging exercise for Data Controllers. According to the GDPR, consent must be freely given, specific, informed, and freely revocable, characteristics that are extremely difficult, if not impossible, to achieve in the complex ecosystems of OBA. Even more demanding is the invocation of consent in special cases involving either minors, who are more vulnerable to manipulation practices and elicitation of consent, or when consent concerns the processing of special categories of data (sensitive data), such as health data or political beliefs, provided of course that their processing is not prohibited by specific legislation (see below Regulation on political advertising and Digital Services Act). Directly relevant to OBA are also the GDPR's provisions

²⁸ J. Ryan, C. Santos, An Unending Data Breach Immune to Audit? Can the TCF and RTB Be Reconciled with the GDPR? (March 23, 2022), SSRN

²⁹ The Biggest Data Breach, Irish Council for Civil Liberties report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe, available at <https://www.iccl.ie/news/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/#:~:text=RTB%20is%20the%20biggest%20data,day%20by%20the%20RTB%20industry>

for the legal treatment of automated decision-making, including profiling³⁰, as the potential application of Article 22 GDPR to online advertising would have significant implications for the lawfulness of processing for these purposes.³¹

Regarding the other available legal bases for processing, specifically legitimate interest and the contract, their invocation may be acceptable in online advertising generally³². However, the characteristics of modern forms of OBA specifically, such as complexity and intrusiveness into users' private lives, raise serious doubts about the suitability of these bases. According to Article 6(1) (f) GDPR, processing is lawful when it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data³³. In the case of OBA, the involved parties should balance their legitimate interests with the rights of users, ensuring transparency and privacy protection, an extremely complex balancing exercise as the intrusiveness of the processing leaves little room for evaluating the legitimate interests of advertisers and advertisers as superior to the fundamental rights and freedoms of individuals. The situation is similar in the case of contracts. According to Article 6(1)(b) GDPR, data processing is lawful when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject

30 According to Article 4 of the GDPR, "profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects of an individual, particularly to analyze or predict aspects related to work performance, financial situation, health, personal preferences, interests, reliability, behavior, location, or movements of that individual.

³¹ Greek Data Protection Authority Guidelines on Automated Decision-Making and Profiling for the purposes of Regulation 2016/679

³² V. Karkatzounis, E. Margaritis, "Contract or Consent for Online Advertising? - A Post-Decision Dilemma in the Wake of the Irish Data Protection Authority's Decision on Meta," DiMEE, 2/2023, pp. 170 - 186

³³ Veale M, Zuiderveen Borgesius F. Adtech and Real-Time Bidding under European Data Protection Law. German Law Journal. 2022;23(2):226-25

prior to entering into a contract. In the case of OBA, it should be documented that the processing is necessary for the provision of services or products requested by the user, such as the provision of targeted advertisements based on their preferences and behavior, which have been agreed through the contract. According to theory and jurisprudence at the European level, this necessity is impossible to document in the context of OBA practices³⁴.

Overall, the GDPR creates a general but strict framework for the protection of personal data, requiring transparency and specific procedures for their collection and processing. These rules catalytically affect online advertising in general and OBA in particular, with the provisions on lawfulness, transparency, data minimization, and security being of greatest interest. Despite the existence of these provisions, their application (or even the possibility of application) in internet practice is called into question, which is also highlighted through the research that will be presented in the second part of this document and is linked both to users' perceptions and business practices.

2.2. The Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector [Directive (EU) 2002/58] and the Proposal for a Regulation on Privacy and Electronic Communications

The Directive on privacy and electronic communications (hereinafter ePrivacy Directive) applies to the processing of personal data in the electronic communications sector, constituting more specific legislation (*lex specialis*) in relation to the GDPR on key issues concerning OBA, such as the use of cookies and related technologies. The central provision of interest from the OBA perspective is Article 5(3) of the Directive, which stipulates that the storage of information or access to information already stored in a device, such as the use of cookies and related technologies like pixels, is prohibited unless the user has given

³⁴ See, for example, the proposals of the Advocate General of the Court of Justice of the EU, Athanasios Rantos, in Case C-446/21 Maximilian Schrems v. Meta.

their consent or when this storage is necessary for the transmission of a communication or for the provision of an information society service requested by the user. In fact, the European Data Protection Board's (EDPB) interpretation of the technical scope is particularly broad and seems to cover every possible means of monitoring user's online behavior³⁵. In simple terms, websites and other parties involved in OBA should ensure clear and informed consent from users before storing or gaining access to cookies and related technologies on their devices. Consent and information should meet the strict requirements of the GDPR mentioned above.

The interaction between GDPR and the ePrivacy Directive often causes confusion, especially regarding the legal basis for processing in OBA. The ePrivacy Directive requires consent for the use of cookies and related technologies, with its exceptions being interpreted very narrowly and only applying to technically necessary cookies, e.g., for security or shopping carts, and not commercially desirable ones, such as traffic analysis or advertising tools. The operation of OBA presupposes the existence of such technologies, therefore consent is necessary in any case, and may also cover subsequent processing operations, for which a legal basis for processing is also required under the GDPR. The GDPR itself in Article 95 states that it "shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in [Directive 2002/58/EC](#)", however, this does not apply in the case of OBA, as the ePrivacy Directive refers to the GDPR for the conditions of consent, which are increased compared to the previous data protection regime (Directive 95/46). Another critical issue regarding the effective regulation of OBA arises from the fact that the implementation of the ePrivacy Directive is left to the Member States, while the Regulation is interpreted and applied more

³⁵ EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

coherently within the framework of the European Data Protection Board (GDPR one-stop-shop mechanism)³⁶.

In light of this analysis, repealing the ePrivacy Directive and replacing it with a corresponding Regulation is a very important and positively anticipated development. The need to clarify the relationship between GDPR and the ePrivacy Directive is emphasized by GDPR itself, while the proposal for the ePrivacy Regulation, even if submitted since 2017, has not yet been finalized. Intense lobbying, the crucial importance of advertising in the Internet economy, and ongoing technological developments are some of the reasons why the effort to establish the new Regulation has experienced such significant delays.

Although the most likely scenario is that there will be significant changes to the final text of the ePrivacy Regulation³⁷, if it is approved, it is worth mentioning some of its basic/key provisions regarding online advertising for the sake of coherence. Regarding the use of cookies and other technologies, the ePrivacy Regulation maintains the existing rule, according to which this is only allowed if the user has given consent that meets the conditions set by GDPR. However, access to terminal equipment is also allowed for other specific and transparent purposes, such as evaluating the effectiveness of a provided information society service, e.g., the service of measuring the number of end-users visiting a website under specific conditions.

Furthermore, the draft Regulation provides that, making access to a website dependent on consent for the use of cookies for additional purposes when there is an alternative instead of payment for access, will be allowed if the provider gives the user the option to choose

³⁶ See in detail Chapter VII of the GDPR and its application to online advertising, specifically in the case of Meta regarding data processing for advertising purposes on Facebook (Binding Decision 3/2022 on the dispute submitted by the Irish SA concerning Meta Platforms Ireland Limited and its Facebook service).

³⁷ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), available at <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>

between that offer and another equivalent offer from the same provider where consent for cookies is not required (existence of a real choice for the end user). The draft Regulation also provides that users will be able to grant their consent for the installation and use of specific types of cookies and other identifiers by selecting one or more providers included in a list of approved providers in the browser settings. The idea of “whitelists” of approved providers aims to address the phenomenon of "consent fatigue" due to the repeated consent that the user is asked to grant for cookies. Consent fatigue can lead to a situation where the end-user no longer reads consent request information, and the protection provided by consent is inevitably undermined and rendered meaningless. Finally, it is essential that - according to the draft Regulation - the processing of cookie data or related technologies will be allowed for a purpose compatible with the purpose for which they were initially collected from the end user's terminal equipment. Factors that will be considered for checking the "compatibility" of the purpose are the connection between the initial purposes and the purposes of the intended further processing, as well as the relationship between the interested end users and the provider. These parameters are expected to play a catalytic role in the future regulatory treatment of OBA.

2.3. Digital Services Act [Regulation (EU) 2022/2065]

The reservations and concerns regarding OBA and the justification for related legislative measures are summarized in just a few lines, in recital 68 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act - hereinafter "DSA"):

"Online advertising plays an important role in the online environment, including in relation to the provision of online platforms, where the provision of the service is sometimes in whole or in part remunerated directly or indirectly, through advertising revenues. Online advertising can contribute to significant risks, ranging from advertisements that are themselves illegal content, to contributing to financial incentives for the publication or

amplification of illegal or otherwise harmful content and activities online, or the discriminatory presentation of advertisements with an impact on the equal treatment and opportunities of citizens". However, the DSA merely reflects a reality - the economic importance of online advertising and the general risks it poses to the privacy and autonomy of internet users - without introducing a comprehensive regulatory system into the legal order.

Recital 69 of the DSA expresses in a careful but clear way the risks of OBA: " When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects." Thus, "targeting" with advertisements based on the specific characteristics of each user - and not just general ones - is something that, according to the EU legislator's perception, can have extremely adverse and harmful effects on the particular (in terms of consumer behavior) psychology of internet users and therefore needs to be addressed and regulated.

However, the DSA regulations do not cover every aspect of OBA. The DSA provisions related to OBA include the complete prohibition of OBA when it is carried out based on profiling as defined in Article 4(4) of the GDPR, using special categories of personal data referred to in Article 9(1) of the GDPR, according to Article 26(4) of the DSA. Additionally, Article 28(2) of the DSA prohibits providers of online platforms from presenting advertisements on their interface³⁸ based on profiling using the personal data of the service recipient when they know with reasonable certainty that the service recipient is a minor. Finally, Article 26(1) of the DSA obliges providers of online platforms that display advertisements on their online interfaces to ensure that, for each specific advertisement presented to each individual recipient, the service recipients are able to identify, in a clear, concise, and unambiguous

³⁸ According to Article 3(m) of the Digital Services Act (DSA), "online interface" refers to any software, including a website or part of it, and applications, including mobile applications.

manner/way and in real-time: a) the nature and purpose of the information as an advertisement, b) the natural or legal person on whose behalf the advertisement is presented, and c) meaningful information directly and easily accessible to the user about the main parameters used to determine the recipient to whom the advertisement is presented and how to change these parameters.

It is not yet clear whether it can be concluded that the prohibition of only specific aspects of OBA, combined with the imposition of special obligations to inform users about its use, makes the use of OBA permissible "a contrario" in cases where it is not prohibited. Besides, the DSA is not the only EU legislative instrument covering aspects of this online advertising technique, while the logic behind its adoption was to ensure and improve the functioning of so-called "intermediaries/ intermediaries service providers" by establishing relevant uniform and mandatory rules.

2.4. Digital Markets Act [Regulation (EU) 2022/1925]

In the same "package" of the Union's acts as the DSA, the Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act—hereinafter "DMA") is also included. The DMA, as EU legislation in the form of a Regulation, is directly applicable in every EU member state and introduces rules for platforms that act as "gatekeepers" in the digital sector. These are platforms that have a significant impact on the internal market, serve as an important gateway for business users to reach their end users, and enjoy, or are expected to enjoy, an entrenched and durable position. What needs to be considered is that gatekeepers often directly collect end users' personal data to provide online advertising services, including when end users use third-party websites and software applications. Additionally, third parties provide gatekeepers with the personal data of their end users in order to make use of certain services provided by gatekeepers in the context of their core platform services, such as customized audiences. Thus, the processing of personal data from third parties using core

platform services for the purpose of providing online advertising services gives gatekeepers potential advantages in terms of data accumulation.

In this way, gatekeepers a) process, for the purpose of providing online advertising services, personal data of end users using third-party services that use the gatekeeper's core platform services, b) combine personal data from the relevant core platform service with personal data from any further core platform services or from other services provided by the gatekeeper or with personal data from third-party services, c) cross-use personal data from the relevant core platform service with other services provided separately by the gatekeeper, including other core platform services, and vice versa, and d) sign in end users to other services of the gatekeeper, unless the specific option has been presented to the end user and they have given their consent within the meaning of the GDPR.

To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they are obligated to allow end users to freely choose to participate in such data processing and linking practices, offering a less personalized but equivalent alternative, without using the core platform service or certain features of it subject to the end user's consent. The less personalized alternative should not be different or of degraded quality compared to the service provided to end users who provide consent, unless the poor quality is a direct consequence of the gatekeeper's inability to process this personal data or introduce end users to a service³⁹.

These provisions of the DMA aim to combat the dominant and monopolistic position that gatekeepers may have regarding the collection and processing of end-user data. These practices seem to need to be evaluated in the context of competition law as well. The German Federal Competition Authority (Bundeskartellamt - BKA) dealt with the

³⁹ D'Amico, Alessia Sophia and Pelekis, Dionysios and Santos, Cristiana and Duivenvoorde, Bram, Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law (March 28, 2024). Utrecht University School of Law Research Paper Forthcoming

compatibility of monopolistic data processing activities with competition law in February 2019. It held Meta responsible for violating EU legislation prohibiting the abuse of a dominant position, regarding practices related to the collection, processing, aggregation, and use of its users' personal data. After an appeal to the German Higher Regional Court of Düsseldorf, that court referred the case to the CJEU. The opinion of Advocate General Rantos dated 20 September 2022 contains interesting thoughts on preliminary questions. The long-awaited verdict of the EU Court⁴⁰ was finally issued earlier this year and confirms the strong relationship between data protection and competition law. Abroad, the U.S. Department of Justice, along with the Attorneys General of various States, filed a lawsuit against Google for monopolizing digital advertising technology⁴¹.

2.5. Unfair Commercial Practices Directive [Directive (EU) 2005/29]

OBA as an advertising technique remains a "commercial practice" within the meaning of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (hereinafter "UCPD") insofar as it aims to promote products and services to consumers.

Judging from the above, undoubtedly the conduct of advertising activities using the OBA technique constitutes an act of "market". It is an activity that has an economic targeting and orientation. Thus, it poses a risk not only to private autonomy or users' informational privacy and, consequently, it does not only concern data protection law. Moreover, it falls more generally within the scope of regulation of private legal relations.

At this point, it is recalled that OBA is not independently regulated by a specific legislation, neither in terms of the conditions for permissible conduct and the rules for its proper

⁴⁰ Judgment of the Court of Justice of the EU in Case C-252/21, Meta

⁴¹ Justice Department Sues Google for Monopolizing Digital Advertising Technologies, available at <https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertisingtechnologies>

conduct, nor in terms of the legal consequences of violations. However, it has recently attracted the attention and increased vigilance of EU bodies, both at research and regulatory levels. While traditional EU advertising legislation mainly regulated the content of the advertising message, setting minimum requirements for professional integrity to avoid abuses, without, however, prohibiting the usual advertising exaggerations that are acceptable in the relevant transaction circle, now the center of gravity is shifting to the recipient of the message. It is inevitable, after all, since "behavior monitoring" for the purpose of shaping consumer consciousness is the quintessence of OBA.

According to the UCPD, "business-to-consumer commercial practices" (hereinafter referred to as commercial practices) means any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers⁴².

However, it is necessary to examine the cases in which the use of OBA as a commercial practice could be considered unfair and on the basis of which provisions given the architecture of the UCPD. Initially, it should be noted that for the purposes of the following analyses, the prior lawful installation of cookies and similar technologies is required as a basic prerequisite for the permissible conduct of OBA, which presupposes, according to what was mentioned above, that there is informed consent as a minimum requirement of the user (see point 2.2. above).

The UCPD protects consumers' economic interests from unfair business-to-consumer commercial practices. It establishes a general prohibition of unfair commercial practices that distort consumers' economic behavior. As such, it also indirectly protects law-abiding businesses from their competitors who do not follow the rules and thus guarantees fair competition in areas coordinated by this Directive. The UCPD provides three stages of

⁴² See Judgment of the Court of Justice of the EU of July 25, 2018, Case C-632/16, Dyson v. BSH, para. 30.

control for assessing the legality and fairness of a commercial practice. Annex I contains the list of commercial practices considered unfair in all circumstances. The same single catalogue/list applies in all Member States and can only be modified by revision of the Directive. If a commercial practice is not "per se" unfair, a second-level check must be carried out. A practice is assessed according to the provisions of Articles 6 to 8 of the UCPD, i.e., whether it constitutes a misleading action or omission, or an aggressive practice, respectively. If the conditions for diagnosing the unfairness of the commercial practice are not met based on the "blacklist" or the specific facts of Articles 6 to 8 of the UCPD, the interpreter and enforcer of the legislation can refer to the "large general clause" and determine whether a commercial practice is unfair due to the fulfillment of the conditions of the general clause of Article 5. We thus have a reverse interpretative and, therefore, applicable course from the specific to the general⁴³.

According to Article 5(2) UCPD, a commercial practice is unfair if it is contrary to the requirements of professional diligence and materially distorts or is likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers. The "average consumer" test applies here, which "is not a statistical test," according to Recital 18. Commercial practices which are likely to materially distort the economic behavior only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way that the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or ones not meant to be taken literally.

⁴³ See Judgment of the Court of Justice of the EU of January 14, 2010, Case C-304/08, Plus Warenhandelsgesellschaft, paras. 41–45.

The purpose of the UCPD is to prohibit such practices that can or could materially distort the economic behavior of consumers, which significantly affect the consumer's ability to make an informed decision, thus forcing the consumer to make a transactional decision that they would not have taken otherwise. A transactional decision means any decision taken by a consumer concerning whether, how and on what terms to purchase, pay in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting.

Section 2, titled "Aggressive Commercial Practices," of Chapter 2 of Directive 2005/29 contains Articles 8 and 9 of the Directive. Article 8 of this Directive, titled "Aggressive Commercial Practices," defines a commercial practice as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.

Article 9 of the UCPD outlines a set of factors to be considered in determining whether a commercial practice employs harassment, coercion, or undue influence. In assessing whether a commercial practice uses harassment, coercion, including the use of physical violence, or undue influence, the following are considered:

- (a) its timing, location, nature or persistence;
- (b) the use of threatening or abusive language or behavior;
- (c) the exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgment, of which the trader is aware, to influence the consumer's decision with regard to the product;

(d) any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader;

(e) any threat to take any action that cannot legally be taken.

Annex I of Directive 2005/29, titled "Commercial Practices which are in all circumstances considered unfair," lists and defines "aggressive commercial practices" in points 24 to 31.

It should be added that, according to Recital 7 of the UCPD, the context of the specific case must be fully considered when applying this directive. This implies an obligation to consider all the features of the trader's behavior in the relevant factual context (Article 8). It should also be noted that the concept of the consumer is of utmost importance when interpreting the provisions of the UCPD. According to Recital 18, the directive uses the average consumer as a reference point, who is reasonably well-informed and reasonably observant and circumspect, considering social, cultural, and linguistic factors. Consequently, a commercial practice cannot be classified as aggressive within the meaning of the UCPD without a thorough and specific assessment of its characteristics in light of the criteria set out in Articles 8 and 9.

Undue influence means exploiting a position of power in relation to the consumer to apply pressure, even without using or threatening to use physical force, in a way that significantly limits the consumer's ability to make an informed decision. The concept of "undue influence," as defined in Article 2(j) of the UCPD, covers the exploitation of a position of power in relation to the consumer to exert pressure, even without the use or threat of physical force, in a manner that significantly limits the consumer's ability to make an informed decision. Undue influence is not necessarily impermissible but is an influence that, subject to its legality, actively involves exerting a certain degree of pressure, thereby compelling the consumer's will.

It should also be noted that Article 8 of the UCPD defines the concept of "aggressive commercial practice," particularly from the fact that it harms or is likely to harm the average

consumer's freedom of choice or behavior concerning a product. Therefore, the consumer must have made a free choice for a service or product to be requested. This presupposes, in particular, that the information provided by the trader to the consumer is clear and sufficient.

2.6. Regulation on the Transparency and Targeting of Political Advertising (Regulation 2024/900)

At the EU level, it has become clear in recent years that the use of targeting and delivery techniques based on the processing of personal data (whether provided directly by users or observed or inferred) is widespread, especially in the context of political advertising. Such techniques can be employed by political advertisers, particularly by very large online platforms as defined in the Digital Services Act, to deliver political advertisements to targeted audiences based on personal data, especially data revealing political opinions and other special categories. As with commercial advertising, the process of monitoring, profiling, and targeting involves the use of algorithms characterized by significant opacity. The potential for misuse of personal data through microtargeting and other advanced techniques is high and is associated with threats to public interests, such as fairness, equal opportunities, and transparency in the electoral process. In this context, it was unsurprising that the European Union, in March 2024, issued a new Regulation (EU 2024/900) "on the transparency and targeting of political advertising."

The new Regulation uniformly addresses a range of issues concerning the transparency and targeting of political advertising related to elections, referendums, or legislative procedures at the EU or member-state level. The rules do not affect the content of political advertisements or other aspects of political advertising, such as the conduct of political campaigns, which remain subject to specific national rules of member states. Among other things, the new rules stipulate that political advertisements must be provided with a transparency label and an easily retrievable transparency notice. They must be clearly identified as political advertisements and must provide certain basic information, such as

the sponsor, the election or referendum to which they are linked, the amounts paid, and any use of targeting techniques. Targeting for political advertising purposes is only permitted under strict conditions. For example, data can only be used after the data subject has given explicit and separate consent for its use in political advertising, while special categories of data, such as data revealing racial or ethnic origin or political beliefs, cannot be used for profiling. Finally, to prevent external interference, the provision of advertising services to third-country sponsors will be prohibited three months before the conduct of elections or a referendum.

3. Conclusions

As demonstrated above, the legal framework for online advertising is complex and multifaceted, with a common focus on enhancing transparency and strengthening user consent. The General Data Protection Regulation (GDPR) serves as the cornerstone of this framework, setting stringent rules for the processing of personal data and aiming to bolster users' capacity for informational self-determination, particularly within complex ecosystems like online advertising. Complementing the GDPR, the ePrivacy Directive addresses specific privacy concerns in electronic communications, including online advertising. However, its effectiveness has been questioned, partly due to inconsistent and problematic implementation across member states. Furthermore, the Unfair Commercial Practices Directive does not explicitly prohibit online advertising based on data processing, even if it involves basic data, but instead sets specific conditions that can only be fully understood through the lens of the GDPR and ePrivacy.

Meanwhile, new European legislations, such as the DSA and the DMA, aim to tighten the rules for digital platforms and enhance oversight of digital markets. The DSA introduces two significant bans on profile-based advertising targeting minors and special categories of data, while the DMA targets tech giants and restricts their ability to engage in monopolistic practices within online advertising. The Regulation on political advertising further tightens the rules for online political advertising, particularly emphasizing transparency. The EU

legislator recognizes the crucial role of targeted advertising in shaping public opinion on political parties and candidates, as well as the risks it poses to society and democracy. It's also noteworthy that, beyond the aforementioned regulations, other legislative acts indirectly relate to online advertising, such as the Platform to Business Regulation [(EU) 2019/1150], the E-Commerce Directive (2000/31/EC), and the Audiovisual Media Services Directive (2010/13/EU).

Overall, the EU regulatory initiatives emphasize the need for user information and consent before processing personal data for advertising purposes. Simultaneously, they stress the importance of informing users and obtaining their consent before installing trackers, such as cookies, for user targeting. However, significant challenges remain in applying and enforcing these rules, particularly concerning the harmonized implementation across EU member states. Despite the EU's coordinated and ongoing efforts, criticism persists, focusing on the increasing complexity and occasional ambiguity of compliance requirements, which can pose a more significant burden on smaller businesses compared to tech giants. Nevertheless, the legal framework includes extensive and strict rules for all aspects of online advertising, such as transparency, consent, and user autonomy (both as subjects and as consumers and citizens), especially regarding the free formation of their choices. Whether legal theory can successfully meet the challenges of online practice is a subject of ongoing research, which will be discussed in detail in the next section.

Part Two:

Perceptions of Users and Businesses regarding OBA

The second part of this research focuses on consumer perceptions and behaviors, as well as business practices concerning OBA and the protection of users' personal data. Therefore, to explore these aspects, we conducted two studies: one quantitative survey targeting consumers and a qualitative survey targeting business employees. The objective was to understand and highlight the corresponding perceptions and practices.

This practical aspect of the research project is significant as it represents one of the few attempts at a European level to document the real-world impacts of legal regulations, particularly for a complex issue like advertising, from an independent and interdisciplinary perspective. Besides, the research has adopted this scientific methodology from the outset, combining a theoretical assessment of the legal framework for online advertising with an evaluation, through surveys and interviews, of how these rules are applied in practice by consumers and businesses.

1. Quantitative Research - Consumer Survey

The sampling was conducted in collaboration with a specialized market research company to gather a random and representative sample that could be generalized to the population. A quantitative survey was conducted using a mixed method of Computer Assisted Telephone Interviews (CATI) and Computer Assisted Web Interviews (CAWI), utilizing a structured questionnaire. Regarding sample selection, the telephone segment of the survey involved random sampling of landline and mobile phone numbers in the survey area, generated through a Random Digits Dialing - RDD process, while the online segment was conducted through an online panel provider. The participants (718 online and 287 via phone) anonymously responded to the questionnaire provided to them. This combination ensures a scientifically sound approach, yielding inclusive and reliable results by not

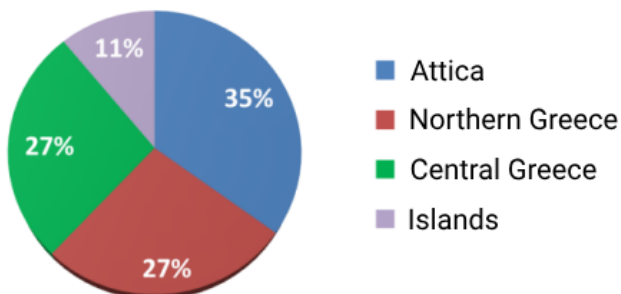
excluding individuals who do not use the internet, either generally or for survey participation.

Quantitative Research - Consumer Survey

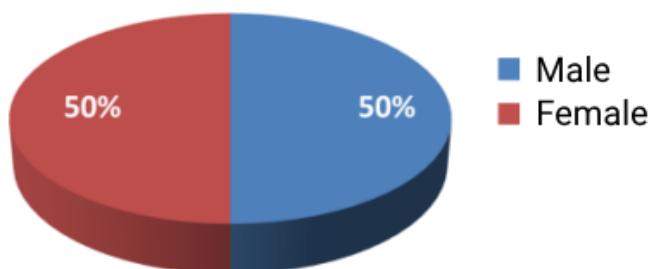
The sample consisted of 1,005 participants, both men and women, aged 18-70 years, residing in Greece. The prerequisites for their participation were internet usage ("Do you personally surf the internet?") and exposure to personalized/targeted advertisements ("Have you seen ads while browsing sites, such as online newspapers, email services, or social media?"). The survey was conducted in February and March 2024.

In terms of sample description, the majority were residents of Attica, with an equal number of men and women. Concerning their age, most participants were 45-54 years old, followed by those in the 35-44 age group. Additionally, most respondents were married and employed.

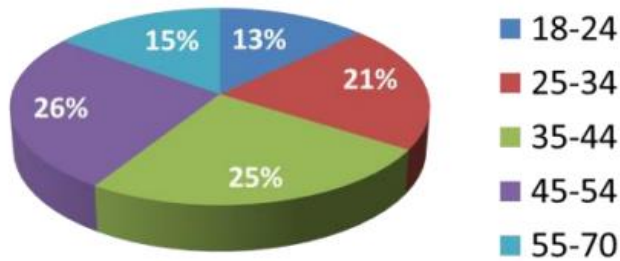
Residence



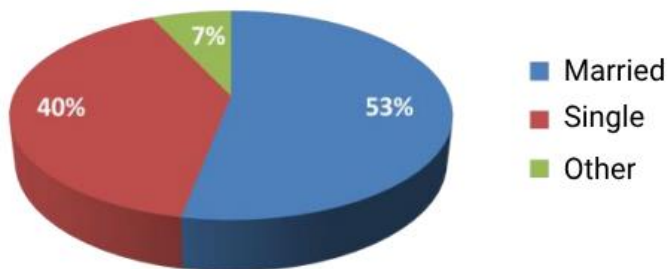
Gender



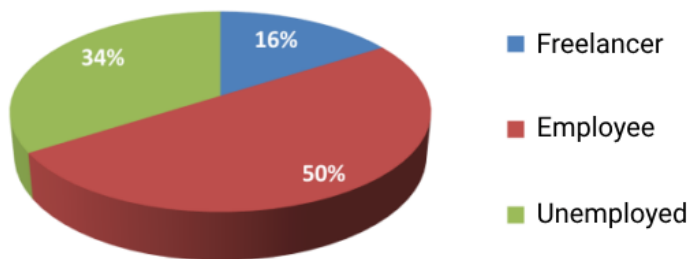
Age



Family Status

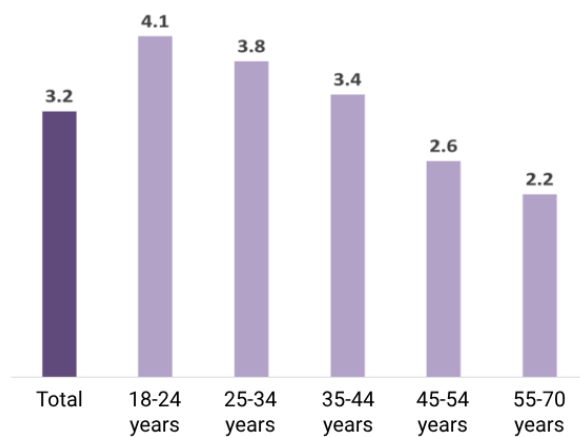
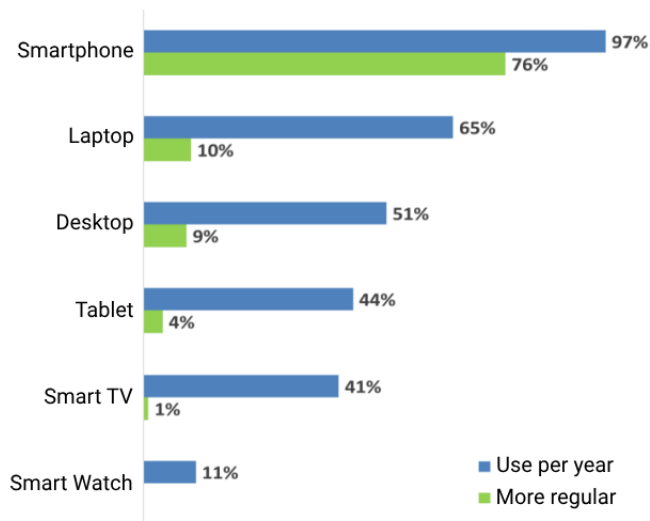


Employment Type



The devices used by participants to connect to the internet were primarily mobile phones/smartphones, laptops, and desktops, with mobile phones being the most frequent device used. The mean daily time spent online exceeded three hours, with a decrease observed with age. These findings are particularly crucial not only for research but also for practical purposes in evaluating the techno-economic parameters of online advertising,

such as the methods of providing information or restricting user access to information based on the medium used, such as mobile phones or desktops.



Average

Personalized ad content, benefits, risks, and intention to provide personal information

Respondents were then asked to answer a series of questions, adapted by the Research Team based on international surveys and academic literature. These specific questions were answered on a 7-point Likert scale (Strongly Disagree 1 - Strongly Agree 7), and below is the mean value (hereinafter "M") of the responses.

At a moderate to high extent, participants stated that they are interested in how and for what purpose their data is collected by the websites they visit, such as web pages, applications, and social media (M=4.8). This element should be evaluated considering the "privacy paradox," i.e., the inconsistency observed between an individual's intentions to protect their privacy and how they actually behave online. Regarding the trust they have in the websites of companies they browse in relation to the management of their personal information, respondents' answers were at medium levels. In relation to how they perceive personalized advertisements and generally the personalized targeting of online advertisements, their responses displayed at moderate to high levels the perception of the nature of this type of advertising. Regarding the perceived benefits that consumers derive from viewing personalized advertisements, participants' responses were equally at a medium level. The above findings show that consumers perceive the personalized nature of online advertisements and recognize the benefits they provide them, but not to a particularly large extent. This leads to the conclusion that companies will need to strive for further actions to highlight how each customer is unique, presenting them with content tailored exclusively to their interests.

Regarding the risks targeted advertising poses to consumers, as perceived by users' evaluation, the responses were at quite high levels compared to the perceived benefits they derive. Specifically, the mean value of concerns for their online privacy was recorded at a moderate to high extent, and their responses to perceived risks were at the same levels.

Regarding the potential insecurity that the practice of displaying advertisements based on their personal data may inflict on consumers, moderate to high levels were noted.

As for the intrusiveness of personalized advertising, participants perceive it to a large extent as "annoying" and "irritating." According to the above results, we observe that consumers have a relatively high degree of concern about companies having access to their personal data, as well as about them processing it in ways that users themselves are not sure they know about, which is why they feel vulnerable. Also, they perceive advertisements containing personalized content as intrusive, which means that the irritation created due to the appearance of such advertisements can lead them to take protective measures, as according to the statistical results of the correlation between these two factors (intrusiveness and behavior for privacy protection) there is a statistically significant relationship.

After evaluating both the positive aspects and advantages offered by online personalized advertising, such as the benefits of saving time from product search and displaying content tailored to consumer preferences, as well as the negative aspects and risks, such as the perceived intrusiveness by consumers and the feeling of vulnerability and insecurity, participants were asked about their intention to provide their personal information in case company websites suggest products or services based on their purchasing behavior, their browsing history on the Internet, as well as their location - when their device's location services are active. The answers they gave recorded medium to low levels, while slightly higher were the answers about their attitude towards this type of advertising and their intention to "click" on the personalized advertisement to receive further information.

Regarding the intention to purchase products and/or services seen in personalized advertisements by the respondents, the mean value of the answers displayed low to moderate levels. Additionally, 9 out of 10 internet users have made purchases online within the last twelve months, while within the same period, 6 out of 10 have purchased products displayed in online personalized advertisements. This data acquires particular value in view

of evaluating the argument of the effectiveness of targeted advertising compared to other forms of advertising, e.g., contextual.

As for their relationship with innovative technologies, the responses of participants belonging to the age categories 18 to 54 recorded the highest mean levels ($M=4$), while between men and women, men's responses recorded the highest mean levels ($M=4$).

Additionally, it is important to mention that respondents stated to a large extent that they had heard/read during the last twelve months about the use and possible misuse of users' personal data on the Internet, with participants aged 55-70 recording the highest mean value ($M=5.1$). To the question about the frequency with which they feel they have fallen victim to privacy violations on the Internet, medium to high levels were average recorded, with men noting the highest mean value ($M=4.3$). These elements are useful in evaluating the level of transparency in how online advertising operates and users' understanding of the risks.

Moreover, it is necessary to mention some statistically significant relationships between the following variables that emerged through this research for consumers. According to the results of the statistical analysis, the trust consumers feel towards companies is positively related to the perceived benefits they derive through the personalized content of advertisements, their intention to provide their personal data to businesses, their attitude towards personalized advertisements, as well as their intention to purchase the products appearing in them.

Additionally, the risks as perceived by consumers involved in providing personal data, as well as users' concerns about the security of their information, affect negatively their intention to share their personal details with companies, their attitude towards personalized advertisements and purchase intention. They are also related to the insecurity they feel and the intrusiveness that, in their opinion, characterizes these specific online targeted advertisements.

Consumer behavior regarding cookie messages

In the next part of the questionnaire, participants were asked to answer a series of questions about accepting/rejecting cookie messages that appear at the beginning of browsing a website. According to the statistical analysis results, almost 1 in 2 participants has been exposed to cookie-related messages and has clicked on them to learn more information, but 2 in 10 of them do not understand the explanations given, while the rest who choose not to read more information do so either because they ignore the ads or because it takes time or because they think they cannot avoid them. Respondents' answers regarding the control they feel they have over which ads appear on the websites they visit were recorded at a moderate to low degree ($M = 3.1$), while it is worth noting that among age groups, the 18-24 category recorded the highest mean value ($M = 3.6$) and participants aged 45-54 recorded the lowest mean value ($M = 2.8$). A possible explanation for the difference between these two age categories could be that young people are more familiar with technology, the internet, and potential risks, and therefore feel they have more control compared to those aged 45-54. This data is extremely useful in evaluating the effectiveness of the theoretical prerequisites set by the data protection and consumer framework on a series of issues, such as consent, information, and consumer decision-making.

Additionally, 72% of participants stated that they have tried to avoid viewing personalized ads at some point, mainly by using Adblockers (55%), deleting marketing cookies (44%), or adjusting options within the ad (43%).

When asked about what elements they believe are recorded by sites, participants stated that these are searches they have made (75%), browsing history (71%), products they have viewed (63%) or purchased (53%), and location (51%). They also mentioned their gender (43%), personal information (43%), interests (41%), age (39%), and IP address (34%), while those who have tried to block ad display believe to a higher degree that all elements are recorded. This data is important for understanding the framework of users' expectations regarding processing their data for online advertising purposes, as well as the technical means they are willing to use to avoid ad display. For 66% of participants, interesting site content plays a role in accepting a personalized ad.

Regarding the measures consumers take to protect their online personal data, the answer that displayed the highest mean value was limiting location services (e.g., Google Maps), while the lowest mean value was recorded for their responses regarding reading the privacy policy of online services and changing default online privacy settings.

Regarding the acceptance or non-acceptance of providing free digital content, such as reading news etc., in exchange for using personal data for advertising, 29% of the survey population responded that it is acceptable, 28% stated that it is neither acceptable nor unacceptable, 26% of participants consider it unacceptable, while 12% answered that they consider it absolutely unacceptable and only 5% consider it absolutely acceptable. However, a limited percentage of the population (27%) would be willing to pay a financial fee instead of providing personal data. Of these, 42% would be willing to pay an average of 17 euros annually for access to a social media platform, while 41% would be willing to pay an average of 18 euros annually for access to a news website.

According to the research results, in the marketing field, businesses should invest in important factors such as "trust" and "brand loyalty" so that consumers feel it is worth sharing their personal data as they receive more benefits. According to Hayes et al. (2021), the existence of a strong relationship and trust between the customer and the business (Customer-Brand Relationship) increases the benefits of personalized/targeted ads as perceived by them and reduces perceived risks, such as data leakage, the feeling of insecurity etc., which can lead them to a greater intention to provide their personal information to companies. Moreover, as the research results showed, when consumers feel that their online privacy is at risk and threatened, they are not willing to provide their personal data to companies, nor to buy the advertised product of the targeted advertisement.

Additionally, another suggestion is to emphasize what the advantages that users can receive through the display of personalized ads are, such as saving time from searching for information, and to emphasize that consumers' personal data on company websites is

secure. Furthermore, given that participants' responses regarding the perceived intrusiveness of personalized ads recorded medium levels, companies could reduce the number of those ads that are displayed repeatedly.

2. Qualitative research - Interviews with businesses

Alongside the research on consumer perceptions and behavior regarding personalized advertisements and their data, a study was conducted on business practices. More specifically, qualitative research was carried out, as the main interest was the in-depth investigation and recording of participants' experiences. The method of personal interviews was chosen with business owners and employees who cater to both B2C (Business to Consumers) and B2B (Business to Business) markets. The participants totaled 9, with an age range from 38 to 55 years old, while in terms of gender, there were 5 men and 4 women.

These particular participants were selected as they had rich professional experience and knowledge relevant to the subject of this research. Before starting the interview, we informed each interviewee about the research topic and assured them that the data would be completely anonymous and absolutely confidential.

Interviewee Profiles

Participant 1 is a Marketing Strategy Leader in an e-shop that employs 25 employees serving both B2C and B2B markets. Some of their duties include monitoring the Key Performance Indicators (KPIs) designed to evaluate the company's marketing actions, monitoring and identifying marketing channels that bring better results, and communicating with the department handling the company's social media.

Participant 2 is the owner of a small-to-medium-sized business - a telecommunications and network provider, which caters to B2B and B2C markets. They have taken charge of the e-shop themselves as they possess high-level programming and marketing knowledge.

Participant 3 is a Marketing Director in a well-known retail company that targets the general public. They deal with both the company's digital marketing (website, social media) as well as traditional marketing.

Participant 4 is the CEO of a technology company that measures the degree of customer satisfaction from stores where they have made online purchases. Due to the nature of the company, the business has in its clientele businesses aimed at consumers.

Participant 5 is a Product Owner at a marketplace operating in Greece, primarily serving the B2C market.

Participant 6 is a Technical Production Director, Founder and Partner of a digital agency that provides consulting services in digital presence, design, and development of the structural needs of each company it undertakes.

Participant 7 is the CEO of an omnichannel marketing automation and content personalization platform that serves retailers with clients in Greece, the rest of Europe, and the USA.

Participant 8 is a Digital Marketer for a small hotel business located on a Greek island, which is a very popular tourist destination. Their main duties include targeted advertising on social media, creating content on platforms where the business has a digital presence, and communicating with the public.

Participant 9 is a Product and Audience Director for a digital publisher company that produces and creates content for news sites. Their main duties are to create products and monitor the results on the site (performance).

Collection of consumer data by businesses

Participant 1, in response to a question about consumer data used by the company, mentioned that it is classified into three categories. In the first category, the company

knows nothing about who the users are on its website, as they may have entered the site for the first time or have not made any conversion, meaning they haven't created an account on the website and/or haven't made a purchase to transform from simple users to customers. The only data the company can extract is what is provided through Google if users have navigated to the site through their Google account. This data can indicate the country they are in at the time of browsing, whether they have connected from a mobile device, as well as their age and gender. The second category of users includes those who have registered on the company's website or newsletters and those who have accepted the terms of use for statistical analysis and promotional activities. In the third category of users, where the company's goal is to lead most consumers, much more data is stored in databases using strong encryption techniques.

According to Participant 2, the consumer data collected is mainly demographic - full name, gender, home address, email address, etc., and collection is primarily done during user account creation for sales and newsletter sending.

Participant 3 mentioned that user data received by the company for online advertising purposes is demographic (e.g., gender and age of consumers) and behavioral (e.g., user habits on the company's site). They explained that specific data such as users' full names can be stored in the database only when they have made a purchase in the company's e-shop and are therefore customers, or when they fill in their personal details in the contact form to receive newsletters with company news and offers, as well as electronic birthday cards.

The company's website, where Participant 4 works, has educational content allowing customers to learn helpful information about its operation. As such, it does not use online personalized advertisements. User data is obtained through a contact form and questionnaire where they are asked to evaluate their experience from the e-shop they purchased from, in order for the business to measure customer loyalty (customer loyalty, voice of customer).

Additionally, Participant 5 told us that the company receives consumer data by asking them for the necessary information to proceed with an order on the site. For example, consumers create a user account by filling in their name, surname, and email address in order to make a purchase on the site.

Participant 6 mentioned that what the company insists on when advising its companies/clients is the importance of obtaining user consent for any action involving their personal data.

Participant 7 stated that most of the data recorded is in anonymous form and comes through Google Analytics.

Participant 8 stated that they receive user data for online advertising purposes from Meta Platforms, where they select the demographic and behavioral characteristics of those to whom they want the hotel business's ads to appear.

Participant 9 told us that the company displays personalized advertisements from other companies on websites using Third-party cookies. It also relies on First-party cookies targeting its own audience.

Privacy Policy

Regarding the privacy policies of company websites, participants mentioned that users are provided with full knowledge of the policy and are asked for their consent to continue browsing the respective company's site. However, they observe that a large percentage of users typically consent without having read all the terms of use or even without opening them. According to them, this happens for various reasons, such as the limited time available to users and the difficulty in understanding some legal terms.

At this point, Participant 7 noted that many of the companies with which his business has collaborated have been found to copy the text of other companies' Terms of Use, often without even changing the company name. Participant 9 mentioned that the Privacy Policy

is available on the site, but user consent is not required to proceed with navigation, as its role is solely to inform the public.

Acceptance and Rejection Messages for Cookies

The e-shop where Participant 1 works installs cookies on the browser during user navigation on the site after obtaining their consent, informing them about the purposes of installation, e.g. statistical purposes, targeted advertising, and remarketing. Precisely, the e-shop displays personalized advertisements to consumers; thus, the installation of cookies is deemed necessary to target specific audiences better. Users who choose to reject cookies can still access the e-shop without restrictions. Notably, even if cookies are rejected, according to Participant 1, the company installs them on the user's browser to obtain specific information about them.

In the case of the e-shop managed by Participant 2, cookies are not placed on users' browsers, as he mentioned that personalized advertising is not relevant to him since his clientele consists of known partners and consumers.

For the e-shop where Participant 3 works, the site uses cookies, requesting user consent for their installation after presenting the purposes, such as marketing activities, advertising, and informational messages about offers. If users choose to reject cookies, they do not face any restrictions in accessing the site.

Regarding the company where Participant 4 works, the site uses cookies to track user requests (e.g., appointment scheduling), service contract implementation, and evaluate optimal services at the transaction level. The site displays a message on the user's screen explaining the reasons for installing cookies and providing an option to accept or reject them. If the user does not accept the installation of cookies on their browser, they can still navigate the site without any restrictions.

Participants 5, 6, and 7 stated that they always request user consent first, explaining the purposes, and do not proceed with cookie installation on the browser if users do not agree.

The company where Participant 5 works collaborates with a specialized cookie company responsible for cookie installation requests, messages, purposes, cookie categorization, and reporting to the business. According to him, even with the rejection of cookies, users can continue browsing the site, with a minor exception being that content from external platforms like YouTube may not be displayed, which was also mentioned by Participant 6.

Participant 8 noted that the company's site does not ask for user consent for cookie installation and does not display any related message to users.

The company where Participant 9 works collaborates with a company that handles the display of the cookie consent message to users. The public is given the option to accept/reject cookies and a "more" option where users can learn more information beyond what is provided in the displayed message. If users reject the cookies, they are not installed on their browser, but they can continue to browse the site without any content restrictions.

Issues regarding personal data security

According to Participant 1, if a user wishes to process or delete their personal data, they can contact the e-commerce manager either by phone or email, despite this never having been requested so far. When asked if there has been a leak of consumers' personal information, his answer was negative, and he said no specific plan exists for managing related crises. Data related to bank account details is absolutely secure, as for any purchase to be made, the company directs the user to the bank's environment. Additionally, only authorized individuals from the business or external partners who sign a contract with the company have access to this data. Data of inactive users, e.g., those who do not open the company's informational emails, is kept in the database for about four years and then permanently deleted.

Regarding Participant 2's e-shop, there has never been a leak of personal data, and there is no plan for managing such a crisis. Access to this data is mainly his own, and if consumers wish to process or delete their personal information, they can contact him either by phone

or email. However, they do not have the ability to access this data themselves and see the data that has been collected, except by prosecutor's order.

Participant 3 mentioned that there has never been a leak of users' personal data as the company he works for prioritizes the security of consumer information, as it would not want to risk the trust shown by hundreds of its customers. If a user wishes to process, delete, or view their data stored in the database, they can contact the company by sending an email without any obstacle.

Participant 4 stated that there has been no recorded incident of personal data leakage of consumers/users in the databases of client companies or the company itself, while informing us that there is a plan for managing such a crisis as well as a plan for informing consumers in case such an event occurs. If they wish, consumers can request the deletion of their personal information, which the company adheres to in practice. Similar responses regarding the ability to process and delete consumer data upon their request were given by Participants 5, 6, 7, and 9, who also mentioned to us that there has never been a leak of their consumers' personal data. At the same time, companies have a plan in case data is leaked. In contrast, the hotel business where Participant 8 works does not have a plan in case users' online personal data is leaked.

Application and compliance with the GDPR

Regarding the legal aspect, Participant 1 mentioned that employees responsible for managing users' personal data attend seminars organized by the company's legal department. He also explained that with the implementation of the General Data Protection Regulation (GDPR), the process of collecting and processing consumer data is done in a stricter framework. However, there is a small margin where the Regulation is not strictly followed, mainly for two reasons. The first concerns the company's profit, and the second relates to the technical difficulty of implementation, as not only Internet users but also marketing department employees face challenges in understanding all aspects of GDPR.

Participant 2 emphasized how significantly the landscape for protecting personal data on the Internet has changed since GDPR came into effect. Companies try to comply with the Regulation, otherwise they risk receiving a fine of even very high monetary value, and therefore do not wish to take such a risk. Consequently, the e-shop informs about the privacy policy it applies.

Regarding the company where Participant 3 works, the legal department frequently organizes seminars for marketers and those involved in public communication (advertising campaigns, newsletters, etc.) so that they know which personal user data they are allowed to use. The company places great emphasis on GDPR and, as he mentioned in the interview, no marketing action deviates from the legal framework.

Participant 4 mentioned that anything related to the personal data of their customers and consumers - customers of those, is done according to the provisions of the General Data Protection Regulation. The business does not have a legal department, but it has a legal advisor who guides it in decisions regarding personal data, storage, and sharing of this data.

Subsequently, Participant 5 told us that the company collaborates with a lawyer (external partner), who informs them immediately about any changes in the legislative framework and advises them appropriately before starting an activity involving communication with the public.

Regarding the responses of Participants 6 and 7, they told us that the legal department of the companies they work for advises them on matters related to the proper management of consumer personal data.

However, it is at the discretion of their companies/clients how they will proceed on this issue, as they have signed such a contract that the businesses are not responsible if their companies/clients act in a way that deviates from what is provided by GDPR.

Participant 8 stated that he has no knowledge of GDPR, as the company has not informed him about it nor given him instructions on how to proceed regarding online personalized advertisements and online communication with the public.

Participant 9 mentioned that the company's legal department informs employees - whose duties include communication with the public and displaying online personalized advertisements - when there is a change concerning the legislative framework for protecting consumers' personal data.

Innovative technologies and future predictions

Regarding innovative technologies, such as Artificial Intelligence (AI), Participant 1 said characteristically that it is "value for money", meaning that it is worth it for a company to invest in such technologies in the personalized content segment, as users save a lot of time from their search for products that may interest them and perceive the business this way as an assistant in their market research by displaying better, personalized suggestions. The company gains customer loyalty, sales, and profit from this. Regarding the future, specifically the next five years, Participant 1 believes that with artificial intelligence, companies will increase the conversion rate of visitors to their website into customers since they will not spend additional time deciding what to buy. For consumers, he mentioned that as time goes by, they will be less interested in who can collect and process their personal data, explaining that new generations use technology and smartphones from a very young age, so they will not pay as much attention because they will prefer to enjoy content that concerns them personally.

Participant 2 believes that in the coming years, businesses will heavily invest in AI, leading them to high profitability since it will produce even more targeted content that they will use in privacy policies for consumer personal data. Companies will specialize in consumer information security issues, while consumers themselves will try to take more robust measures against possible breaches of their data. Regarding a potential threat to users' online privacy from AI, he characteristically states that "every coin has two sides",

explaining further that it depends on the company itself how it will utilize the technology and for what purposes.

Participant 3 believes that new technologies will not threaten consumers' online privacy, as it is primarily up to the users themselves whether they choose to share their personal data in order to receive content that matches their interests. The company he works for is going to use artificial intelligence shortly to display suggestions to users that will match their preferences either on its website or in online personalized advertisements.

Participant 4 believes that the situation with online privacy protection will not change immediately from both consumers' and businesses' sides, and neither will artificial intelligence be dangerous for users' personal data. He suggests that the state undertake educational seminars for businesses to ensure that GDPR is 100% implemented.

Participants 5, 6, 8, and 9 believe that technologies such as Artificial Intelligence will not threaten consumers' online privacy, while in their opinion, the future of personal data protection from consumers' side will not change, as they have now accepted that businesses have access to all their information. From the businesses' side, they stated that as the noose tightens in relation to laws, they will become even more careful in order not to risk receiving fines and penalties.

In contrast to what the above Participants mentioned, Participant 7 believes that Artificial Intelligence will threaten consumers' online privacy to a considerable extent, emphasizing tools such as chatbots, for which users should be particularly careful about the information they share. In the company where he works, there is a coordinated effort to focus on the ethical side of AI, which will respect users' personal data and ensure that no one feels that their information is being violated.

Part Three:

Evaluation of findings and guidelines

The third part includes both the evaluation of findings arising from the two previous stages of research (analysis of the legal framework and perceptions of its practical application) and guidelines for the involved parties aimed at more effective protection of users/consumers. The goal of the third part is, among others, to identify problematic aspects of the existing legal approach in digital practice, combined with consumer and business expectations and aspirations, and to raise awareness about these issues.

1. The intractable issues of OBA

A. OBA, consent and transparency: From legal theory to online practice

The evaluation of online advertising regulation leads us to two fundamental conclusions. On the one hand, despite its pivotal role in the digital economy, OBA poses major, and in many cases intractable or even insurmountable problems in terms of data protection, privacy and consumer protection, practically undermining personal autonomy, the smooth functioning of the economy and the integrity of public discourse and democratic processes. On the other hand, OBA has become an integral part of business models within the Internet ecosystem, from "very large online platforms" and "gatekeepers" to small and medium-sized businesses and news websites. To this extent, any regulatory initiative, such as the complete ban of OBA⁴⁴ or the promotion of alternative advertising models⁴⁵, should be

⁴⁴ Bennett Cyphers and Adam Schwartz, "Ban Online Behavioral Advertising", Electronic Frontier Foundation

⁴⁵ European Data Protection Supervisor, Opinion 1/2021 on the Proposal for a Digital Services Act.

made after a proper assessment of the advantages, impacts and side effects for users, society and the Internet⁴⁶.

Data protection and privacy issues in OBA are complex and multidimensional, but for practical and substantive reasons, the main ones identified are the conditions and validity of user consent, transparency and the allocation of processing roles regarding the involved parties.

Consent is one of the cornerstones of GDPR and the ePrivacy Directive, and it should be freely given, specific, informed, and freely revocable. This means that users must fully understand how their data will be used before giving their consent. However, in practice, the process of obtaining valid consent presents significant challenges. Often, the information provided to users is complex and difficult to understand, preventing meaningful comprehension and conscious and freely revocable consent, especially within a vast ecosystem like OBA. The problem is exacerbated by the fact that many users provide consent simply to gain access to desired services, without examining the details, turning consent into a formal procedure or even a trade-off, instead of a substantive act of information and clear indication of will. Proving the obtainment of valid consent also presents challenges, especially given the extensive use of consent management platforms that implement questionable legality protocols, such as TCF⁴⁷.

At the same time, transparency, which is also a central axis of data protection and privacy law, ensures that users are fully informed about how their data is collected, stored and used. However, achieving this transparency is extremely difficult in online practice, especially where OBA involves real-time auctions of users' personal information in complex

⁴⁶ V. Karkatzounis, L. Mitrou, A. Vorras, *Regulating AdTech: Chasing Chimeras or the Art of the Possible?*, Proportionality in EU Digital Law - Balancing Conflicting Rights and Interests, Bloomsbury Publishing

⁴⁷ The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR, available at <https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdp>

and often opaque ways. Moreover, purpose specification, security and data minimization are legal requirements that face inherent difficulties that are inextricably linked to the systemic characteristics of OBA, such as the large number of involved parties. The problems are compounded by the continuous evolution of technology, including the use of artificial intelligence, which enhances user profiling capabilities without their full awareness, potentially undermining their trust and the level of protection of their rights⁴⁸.

Regarding the determination of processing roles in the OBA value chain, this presents very significant challenges. A characteristic example is RTB, where a vast number of advertisers, publishers, intermediaries for consent management (Consent Management Platforms) and data brokers participate, who must define in a documented manner what role they perform in processing user data, to assess their responsibilities and obligations based on the legal framework. According to the criteria set by the GDPR, the EDPB⁴⁹ and the Court of Justice of the EU⁵⁰, in data processing through trackers for online advertising purposes, the most appropriate scenario seems to be that of multiple joint controllers⁵¹. Ad hoc and in-depth assessment of each case remains necessary, especially regarding the delimitation of liability between parties, but it can prove particularly complex due to the complexity of the OBA ecosystem or ineffective for the protection of user data⁵².

⁴⁸ Karkatzounis, V., Mitrou, L., Online Advertising and Data Protection, DiMEE, 1/2020

⁴⁹ Guidelines 07/2020 on the Concepts of Controller and Processor under the GDPR, available at https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_el.pdf, as well as Opinion 2/2010, especially p. 12.

⁵⁰ See, in particular, the decisions of the Court of Justice of the EU in Cases C-210/16 *Wirtschaftsakademie*, C-40/17 *Fashion ID*, and C-604/22 *IAB Europe*.

⁵¹ Joint controllers exist when two or more controllers jointly determine the purposes and means of processing, without this implying that the responsibility held by the controllers is equivalent. See also Article 26(1) of the GDPR.

⁵² As noted by Advocate General Michal Bobek in Case C-40/17 before the CJEU, it is very likely that the person who should bear responsibility for a specific action, i.e., the person exercising substantial control,

The above issues, combined with other aspects of data protection law, are increasingly occupying legislators, supervisory authorities and courts. During the period of this research, significant legislative and jurisprudential developments took place, raising questions about compliance with data protection rules in OBA and the effectiveness - but also proportionality - of targeting practices, while various alternative approaches for milder and more privacy-friendly forms of advertising, such as contextual⁵³, gained ground in public discourse.

At the same time, market-level initiatives have been taken, aimed at better aligning OBA with the data protection framework. Characteristic examples are (a) the new version of the Transparency and Consent Framework (TCF 2.2) of the Interactive Advertising Bureau (IAB), which was issued after the decision of the Belgian authority that ruled that this framework does not comply with the GDPR⁵⁴ and (b) Privacy Sandbox, an effort by Google to develop a more privacy-friendly advertising ecosystem⁵⁵. However, both in terms of privacy⁵⁶ and in terms of interaction with other areas of law, such as consumer law and competition law, these initiatives are still being scrutinized for their completeness, but also whether they

could hide behind all these so-called 'joint controllers,' leading to a significant weakening of effective protection.

53 Karkatzounis, L. Mitrou, Ap. Vorras, The application of the principle of proportionality in the online advertising ecosystem, EFAPOLD, 8-9/2023.

⁵⁴ See footnote 41.

⁵⁵ <https://privacysandbox.com/>

⁵⁶ See, for example, the recent announcement by the French data protection authority titled 'Online advertising: CNIL prepares for changes in business models,' available at <https://www.cnil.fr/fr/publicite-en-ligne-la-cnil-se-prepare-aux-evolutions-des-modeles-daffaires>"

conceal practices restrictive of competition, which would further strengthen oligopolies in the relevant markets⁵⁷.

It is evident that we are going through a transitional and fluid era in the regulation of new technologies in general and online advertising in particular. The future of OBA regulation is based on a blend of interventions, consisting of measures to enhance user autonomy, such as improving certain aspects of consent, and more interventionist measures to protect individuals and society, such as introducing horizontal prohibitions. OBA has proven to be more than just a new form of advertising, so legislators should reconsider their approaches and possibly explore co-regulation and self-regulation models to maintain balance in online advertising ecosystems. Many of these elements are reflected in new EU legislative initiatives, such as the DSA and DMA, and can prove very useful, but their effectiveness will be evaluated in practice. The same applies to the draft ePrivacy Regulation, with its multi-year delay in issuance being an undeniable witness to the complex nature of the issues under consideration and the conflicts of interest in the online advertising sector.

OBA demonstrates that in some cases, the perception that law can keep pace with technological development is practically utopian, especially as conventional tools and legislation methods face severe difficulties in addressing the innovative and complex relationships arising from technological developments. Indeed, while the increasing use of Artificial Intelligence (AI) can be beneficial for the business model of the involved parties, it simultaneously exacerbates existing challenges and creates new ones for the effective implementation of the legal framework.

The trends of the modern Internet economy, the increasing volume of information, and the rapid technological evolution seem to inevitably lead to the market's transition from programmatic to algorithmic advertising. Protecting personal data and privacy in online

⁵⁷ D. Geradin, D. Katsifis, Taking a Dive Into Google's Chrome Cookie Ban (February 19, 2020). TILEC Discussion Paper No. DP2020-042

advertising is an ever-evolving challenge that requires coordinated efforts from legislators, businesses, and users. As the European Data Protection Supervisor notes, today's internet situation is not "set in stone" - on the contrary, it is a product of human and political choices⁵⁸. In this context, the re-approach to consent, enhancing transparency, and effectively exercising data subjects' rights, especially in light of profiling and automated decision-making, are catalytic factors in shaping a safer, more transparent, and functional online advertising ecosystem.

B. Could OBA be classified as an aggressive commercial practice?

To determine under what conditions OBA will fall within the scope of the UCPD and thus constitute an unfair commercial practice, in the form of an "aggressive" commercial practice under investigation, we must examine whether OBA can force the consumer to make a "transactional decision." According to the wording of the Directive, "any decision taken by a consumer concerning whether, how and on what terms to purchase" is a transactional decision. Therefore, this concept covers not only the decision to purchase a product or not, but also the decision directly related to that decision, especially the decision to enter the store. According to the CJEU, the term "transactional decision" is a legal concept that can be interpreted in many ways and is broadly defined. Thus, in the context of the digital world, "clicking" on an ad falls under the above concept. In reality, and considering the wording of the UCPD, all advertising practices fall under the term "transactional decision."⁵⁹

Who is the "average consumer" in the context of OBA, which, as mentioned, can be permissibly performed only when there is first user consent, according to Article 6(1) of the GDPR? Is it reasonably expected that the average consumer will act rationally, being

⁵⁸ W. Wiewiórowski, It is time to target online advertising, European Data Protection Supervisor 64

⁵⁹ See in detail E. Margaritis, Online Behavioral Advertising as an Aggressive Commercial Practice *Journal of European Consumer and Market Law*, Volume 12, Issue 6 (2023) p. 243 mainly pages 248 επ.

"reasonably well-informed, observant and circumspect," as mentioned in recital 18 of the UCPD?

The answer is ontologically and empirically negative. The average consumer is unlikely to be interested in meticulously reading the long and multi-layered "privacy notices" or "cookie policies" of their visiting pages. Even if he or she is willing to do so, they will be lost - as "uninitiated who are unfamiliar with the terminology" - in large and ambiguous details of the "partners" providing cookies, vague descriptions of processing purposes, abstract statements regarding the functionality of each cookie or the duration of its operating period. The average consumer can, on the contrary, be reasonably informed when the cookie functionality statement is simple even through visualization, with concise and defined references to the possibilities of exposure to retargeting based on their data that will be observed through algorithmic functions⁶⁰. To satisfy this requirement, the initial cookie statement can be combined with the information resulting from the relevant provisions of the DSA. That is the obligation to inform the user about the main parameters used to determine why they were chosen as a recipient to whom an advertisement would be presented and how to change these parameters. And, of course, no cookie placement should be made unless the user has given prior consent, in accordance with the provisions of Article 5(3) of the ePrivacy Directive.

If the consumer has this information, then they can be characterized as aware that they are being targeted. And only then will they be able to truly realize that they may be the "product" for the free use of a service. However, if targeting is conducted without meeting the formal requirements for the lawfulness of processing, then according to the view expressed herein, OBA will undoubtedly constitute an aggressive commercial practice.

⁶⁰ J Laux, S Wachter, B Mittelstadt, 'Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice' (2021) 58(3) Common Market Law Review, pp. 6 – 7.

OBA is inherently structured to act as a catalyst in exploiting human emotions. Extensive machine learning capabilities, real-time user profile analysis tools, creating digital personalities for each of them that will be revealed to intermediate advertising agents, expose every data subject and, one might say, "digitally vulnerable." All thoughts, searches, cognitive failures, biases and cognitive axioms, fears and desires can be analyzed and utilized. This exploitation of psychological characteristics through the distraction of attention, the elicitation of information about an individual and its use to influence the consumer's self-determination is what rings the bell for the evaluation of the unfair influence criterion.

So, could OBA be categorized/under conditions as an aggressive commercial practice under the prism of the UCPD? As a general rule, when exercising an aggressive commercial practice, according to the analogy behind the UCPD, the trader exploits the consumer's weak position, abusing a position of power that has been illegally acquired - through harassment, coercion, physical violence or proactive influence. This results in harming the consumer's freedom of choice by inducing them to enter into a contract or otherwise make a transactional decision that they could have avoided if this illegal advantage did not exist. And this is precisely evident in the case of OBA, where each user's profile, which reveals their vulnerabilities, in the means of preferences and inferred characteristics, is used to present them with personalized content in such a form that it is shaped as "unjustified influence" when monitoring is illegal.

The essence of OBA itself is the cognitive imbalance between the trader and the consumer, which could be characterized as "undue influence." The trader truly understands the consumer's characteristics and exploits them to generate revenue by targeting the consumer with relevant content. This is why OBA is employed in the first place. Modern behavioral economics suggest the use of "customized" rather than general advertising. This "awareness" is the most critical factor in classifying OBA as an aggressive practice, as the trader (whether they are the cookie placer or the third party to whom data is disclosed after cookie placement) uses the data to deliver personalized content. Cognitive or behavioral

weaknesses are susceptible to the trader's ability to determine what might activate the consumer's harm in terms of bending their unimpeded will to make a rational transactional choice.

Of course, awareness of undue influence is not the only criterion for confirming a commercial practice as aggressive. There are many variables that, according to Article 9 of the UCPD (Unfair Commercial Practices Directive), must be considered to assess whether a commercial practice is based on undue influence. Among other things, it is essential to mention, as part of a non-exhaustive list, the timing, location, nature or persistence of the practice, the language used, the adopted behavior, the exploitation of any misfortune, or the imposition of burdensome or disproportionately unconventional obstacles.

The final criterion for confirming the exercise of undue influence should be evaluated: the exercise of power. It should be acknowledged that power does not need to be interpreted through the lens of competition law. It is, however, undeniable that technological giants, who have taken on various roles in the AdTech sector, acting simultaneously as publishers and intermediaries, tend to accumulate a large volume of data which their analytical tools allow them to further process and use for revenue generation, thereby capturing a significant market share. As mentioned earlier, the DMA will act as a barrier to combining data from various core platform services unless user consent is provided. However, this does not seem to apply here. "Power" must also be understood in a realistic way, along with the undeniable economic imbalance between the parties, as the informational position that gives the trader the advantage of targeting the consumer without the consumer's consent. It is a "mental" dominance, as Galli puts it⁶¹. This interpretation of power is supported by the flexibility of the UCPD's phrasing to address recent marketing models that were not widespread at the time of the UCPD and its ability to adapt to the current online

⁶¹ Galli, Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD. In: Ebers, M., Cantero Gamito, M. (eds) Algorithmic Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law, vol 1. Springer (2021), 125

economy. This concept aligns with the fact that "power" should be understood in such a way that online advertising goes far beyond simply "prompting" the user to make a transactional decision, but rather appears as manipulation and a violation of privacy.

One might argue that this view is somewhat paternalistic. That not every form of OBA has the capacity to manipulate rational abilities or distort the average consumer. However, the view presented here undoubtedly has a strong point. By assessing each form of OBA that does not meet the legal data processing requirements as aggressive, a significant alignment is achieved, namely, the alignment of the regulatory data landscape with market-oriented consumer protection provisions. Of course, these legal "universes" do not always intersect, but they are at least compatible.

No one can dispute that in the modern data-driven economy, the necessity for a universal legal regime could serve the best interest of the "consumer as a user," a new type of digital subject surfing the web and subjected to ubiquitous monitoring. Suppose this desired goal raises the thresholds for lawful monitoring, so that many business practices are not compliant when assessed against the UCPD criteria. In that case, it results from applying the relevant provisions according to recent privacy amendments and not a premise needing verification. The decision of the CJEU (Court of Justice of the European Union) in Case C-646/22 regarding the concept of the average consumer in the digital age is awaited – would this trigger a shift from the "home economy" model to the "homo interneticus" model?

C. Data as Counter-Performance?

The boundaries between OBA (Online Behavioral Advertising) as the dominant business practice in the data-driven economy and illegality from the perspective of unfair business practices (whether consumer-related or on a B2B basis) are neither clear-cut nor easily understood. According to the current legislative framework, which stipulates that informed consent must be given before monitoring, it would likely be impossible to avoid condemning OBA as illegal under data protection laws. However, this also reflects the assessment of this

commercial practice as unfair due to its extensive potential to subtly manipulate rational behavior, from the consumer protection law standpoint.

Behavioral targeting poses a threat not only to individual and transactional autonomy and freedom of decision-making but also to democracy itself. Notably, the EU has recently taken legislative initiative in the form of a regulation proposal on transparency and targeting of political advertising. To address the new challenges posed by online electoral campaigns, the European Commission has proposed a harmonized set of rules regarding transparency and targeting of political advertising. These rules will apply to both online and offline political advertising. The proposal is currently under discussion in the European Parliament and the Council, according to the usual legislative process, with the aim of "addressing manipulative interference."

But can all revenue-generating techniques based on data be deemed illegal in our time? Recently, the adoption of Directive (EU) 2019/770 of the European Parliament and Council, dated May 20, 2019, regarding certain aspects of contracts for the supply of digital content and digital services (DCD) recognizes that digital content or digital services can also be provided when the consumer does not pay a monetary price but provides personal data to the trader, with such business models being used in various forms across a significant portion of the market. The European legislator refrains from fully recognizing personal data as counter-performance to avoid categorizing it as a tradable commodity. Therefore, the relevant provisions of the DCD appear to regulate only the "provision of active data" in exchange for the trader's performance.

In any case, the "payment with data" model is expected to prevail in the coming years. What the boundaries of lawful data processing will be in such cases, and how the existing legislative framework could be applied to the new data economy, is something that needs to be further examined and developed. And a question for future consideration: Could "contractual performance" be characterized as a lawful basis for data processing in "walled gardens"? Moreover, how legally, ethically, and psychologically mature are we as legal

stakeholders to transition to the next model, that of “Pay or Okay,” where targeting with advertisements is not merely a “side effect” of accessing a website but becomes a form of counter-performance? Or, in legal terms, does access to a digital service (application, website, platform) directly correlate with the “provision” of personal data by the consumer, such that refusal to provide it could be a reason to terminate access to a digital service⁶²?

2. Guidelines

After completing the evaluation of the findings from the previous two stages of the research (legal framework analysis and perceptions of its practical application), the research team proceeded to develop guidelines for three distinct target groups: internet users, who are the recipients of online advertising; businesses involved in the online advertising value chain; and regulatory authorities (data protection, consumer protection, and others) tasked with ensuring the legality of online advertising.

1. Internet Users

The research findings clearly indicate limited awareness among internet users regarding how online advertising operates and the risks involved. Therefore, raising awareness among users about online advertising and micro-targeting is of crucial importance. The research team believes that an informed user can more effectively assert their rights both as a data subject and as a consumer.

The five (5) guidelines for internet users are as follows:

i. Awareness

Online advertising is a complex and opaque ecosystem in which users should remain vigilant and informed about how they are targeted by advertisements, who is targeting them, and

⁶² EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

how their data is used for this purpose. It is essential for users to check the terms of use, read privacy policies, and review permissions when using online services. The information provided to users should be easily accessible, understandable, and in clear and straightforward language. Often, helpful information is provided in banners when visiting a website, which users might overlook out of habit or fatigue. Attention should be heightened when online advertisements lead to transactions, for which users should receive as complete and understandable information as possible before completing them.

ii. Consent

Consent is internet users' primary tool to control their data, protect their privacy, and self-determine their information. User consent is essential for OBA (Online Behavioral Advertising), mainly due to the installation of trackers on their devices. Often, users are accustomed to trading their data for access to services; however, in many cases, the trade-off is disproportionate, involving continuous attention and time spent on websites and online services. Therefore, user consent should be given only when users are assured of their data's security and lawful processing. Additionally, users should be cautious about recognizing dark patterns that attempt to extract their consent unfairly, such as through color and font choices⁶³.

iii. Verifying information and Rewarding Good Practices

The internet is a vast environment with a massive volume of information, much of which is inaccurate or misleading, whether unintentionally or deliberately. Internet users are constantly exposed to content and advertisements, the reliability of which should be continually checked. It is crucial for users to have the means to verify the credibility of advertised products, services, or content before making decisions (e.g., purchasing a

⁶³ C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)

product or subscribing to a service). Simultaneously, users should reward services and websites that handle their data responsibly and provide reliable content. Utilizing privacy protection tools, such as privacy-friendly services and software, and reviewing privacy settings provided by services can be particularly useful.

iv. Protecting Vulnerable Users

If managing personal information online is difficult for the average user, it is even more complex for vulnerable groups, such as minors and the elderly. These groups might have less awareness of risks, consequences, and consequently, the guarantees and rights related to their data processing for online advertising purposes and profiling based on their online activity. The legislative framework recognizes these issues and imposes stricter conditions for their information and consent. However, in practice, it is crucial that these individuals receive support from their caregivers when using the internet, whether through technical means, such as privacy protection measures in apps and browsers, or through clear explanations of the information they receive.

v. Exercising Rights

The legislative framework at both national and EU levels provides a range of rights for the protection of internet users in the context of online advertising. However, a key factor in the effectiveness of this legal framework is user awareness of their rights and how to exercise them effectively. Users should be informed about the options provided by platforms for reporting inappropriate or misleading ads, exercising their rights, such as accessing data used for advertising purposes, and how to file complaints with the relevant supervisory authorities.

From ads that discriminate against them or are intrusive to ads that use misleading practices to lead them to a transaction, users should be aware and able to exercise their rights, whether as data subjects, consumers, or citizens.

2. Businesses

The research demonstrated that the role of businesses involved in the online advertising value chain, such as websites, platforms, and intermediaries, is crucial in mitigating user risks. Furthermore, proper management of personal data and privacy protection enhance a company's reputation and credibility, as users prefer to engage with companies that respect their privacy and handle their data responsibly. Therefore, the research team considers it essential to inform these businesses about the operation and legality of the practices they adopt, in order to understand the legal risks associated with these practices from the perspective of data protection, privacy, and consumer rights.

The five (5) guidelines for businesses are as follows:

i. Transparency

Internet users have the right to receive clear and easily understandable information regarding the processing of their personal data for advertising purposes. Transparency should cover every stage of processing by a business, depending on the activity it undertakes, and can be implemented through best practices such as readable policies, disclosures, and informational mechanisms. For example, the owner of an informational website or an online store is responsible for informing users at every step of the advertising process, whether conducted by themselves or partners, such as social media platforms or advertising networks they have contracted with. Therefore, the obligation of transparency also includes ad auctions (data used and criteria applied) as well as the algorithms used for ad targeting.

ii. Consent Mechanisms and Exercising Rights

Similar obligations to transparency accompany obtaining consent from users. Involved businesses should adhere to strict rules and robust mechanisms for obtaining and managing consent, ensuring the legality of data processing for advertising purposes and allowing users to retain control over their data. In this regard, utilizing mechanisms that allow users

to easily manage their consent and data (privacy dashboards, consent management systems) is beneficial. Businesses should avoid using "dark patterns" and design consent forms and interfaces in a way that does not mislead or coerce users into unintentional choices. Additionally, they must be particularly careful when selecting their partners, as the security of processing depends on them, without absolving businesses of their responsibilities.

iii. Compliance with Data and Consumer Protection Consumer Laws

Data and consumer protection rules in the context of online advertising are numerous, strict, and continuously evolving. Businesses should make systematic efforts to stay informed about their obligations and have a clear plan for their proper implementation. In this context, they should create suitable conditions for cooperation between those involved in their commercial and technical activities and their legal support team. A thorough understanding of the rules and their integration (from the design phase) into each business's services is crucial for compliance with existing rules and quick adaptation to new ones. Defining the relationship between businesses and major platforms dominating the online advertising sector is also essential to ensure a fair distribution of responsibilities based on their roles.

iv. Protecting Vulnerable Groups

The legal framework for data protection and consumer rights provides special treatment and increased security measures for vulnerable groups, such as minors or the elderly, especially those unfamiliar with new technologies. Businesses should be cautious when engaging in data processing for advertising purposes involving such groups, avoiding targeting ads at them and not exploiting their vulnerabilities. The same applies to individuals or social groups with specific characteristics that fall under the "special" data categories defined by GDPR, such as religious or political beliefs and sexual orientation. Businesses should be aware of their increased obligations when processing sensitive data

for advertising purposes, particularly any prohibitions introduced by legislation, such as the prohibition on advertising based on profile building using special data or data about minors.

v. Regular Audits of Data and Business Models

Every business operating online engages, to a greater or lesser extent, in processing user data, including for advertising purposes. Whether it is an e-commerce store, an informational website, a platform, or an advertising company, user data is central to the business model of the Internet economy. Given the importance of data to businesses and the risks posed to users by improper data processing, companies should place significant emphasis on developing appropriate strategies, structures, and policies for lawful data use for advertising purposes, involving both employees and partners in these processes from the outset. Beyond initial planning and implementation, conducting regular and comprehensive audits and inspections of targeting systems and data sets is equally important.

ii. Consent Mechanisms and Exercising Rights

The research findings clearly indicate limited awareness among internet users regarding how online advertising operates and the risks involved. Therefore, raising awareness among users about online advertising and micro-targeting is of crucial importance. The research team believes that an informed user can more effectively assert their rights both as a data subject and as a consumer.

3. Supervisory and Regulatory Authorities

Supervisory and regulatory authorities generally face an uneven battle in protecting personal data and consumers. They are tasked with highly demanding responsibilities, ranging from raising user awareness and market oversight to conducting audits and ensuring the development of a fairer and more transparent online advertising ecosystem. However, they often lack the necessary resources to effectively meet these challenges. Consequently, the research team considers it crucial to support them in terms of

infrastructure and personnel, as well as through contributions from the scientific community, such as this study, to provide a comprehensive and up-to-date legal analysis of the issues and recommendations that may be useful in the performance of their duties.

The five (5) guidelines for regulatory authorities are as follows:

i. Targeted and Ongoing Sampling Inspections

The value chain of online advertising is characterized by significant power imbalances, not only between users and businesses but also among businesses themselves. The technological giants that underpin the ecosystem are technically and legally difficult, if not impossible, to regulate by a single national authority, especially in smaller member states. However, national authorities could focus on targeted and systematic inspections of larger websites and platforms. These sites receive the highest traffic; thus, ensuring compliance with online advertising laws could have a greater impact on protecting user rights, both data subjects and consumers. Such inspections should be stringent, continuous, and comprehensive, ensuring compliance with the legislative framework without introducing discriminatory practices that disrupt business competition. Inspections can be carried out both independently and in collaboration with other regulatory and supervisory authorities, such as those involved in enforcing the Digital Services Act and the Digital Markets Act.

ii. Collaboration with the Market to Improve Existing Models and Promote Alternative Advertising Models

Beyond inspections, the market at the national level requires guidance and support from authorities to improve existing models and develop new advertising models that are legally compliant and more privacy friendly. Supervisory and regulatory authorities can engage in a more systematic dialogue, possibly through a forum, and collaborate with other relevant authorities and the market to promote best practices. For example, this could include enhanced protection for minors, avoidance of harmful practices like misleading design, and prevention of systemic risks such as user manipulation. Although resources for authorities are limited, their role in encouraging all stakeholders to adopt standards, models, and codes

of conduct is not only a legislative imperative but also a necessary path for identifying sustainable alternatives in online advertising.

iii. Collaboration with the Scientific/Research Community

Equally important as ongoing interaction with the market is the collaboration between supervisory and regulatory authorities and the scientific and research community. Regulatory authorities can benefit from researchers' high level of expertise and specialization, either through bilateral collaborations or within the framework of broader research programs at the national and EU levels. Rapid technological and legal advancements in the Adtech field require continuous updates, heightened vigilance, and in-depth analysis, which are attributes characteristic of the scientific and research community. Conversely, the community could gain from the practical experience of regulatory authorities. Additionally, authorities could leverage partnerships with research institutions to meet legislative goals and obligations, such as by providing incentives for the recognition of vetted researchers within the framework of the Digital Services Act.

iv. Training and Awareness

Training businesses and raising user awareness are critical factors in ensuring the legality of online advertising. The role of supervisory and regulatory authorities can be particularly significant in these processes. From conducting targeted seminars and events to creating and promoting informative materials and disseminating them online, regulatory authorities can help enhance transparency in online advertising and improve the level of information available to all involved parties. Businesses can utilize such official materials for employee training, while users can receive accurate, relevant information in a user-friendly, understandable, and reliable manner. In this way, authorities can contribute to building overall trust between users and businesses based on transparency and accountability.

v. Submitting Proposals for Shaping the Legislative Framework

The evolution of the legislative framework at the EU level is rapid and multi-layered, aiming for the harmonization of rules through legislative tools such as Regulations, which have direct applicability in member states. However, in certain cases, there is room for initiative either during the transposition of Directives, such as the ePrivacy Directive, or in their interpretation, such as the Directive on Unfair Commercial Practices, supported by the scientific interpretation in this study, or in taking national initiatives that do not disrupt the single digital market. For instance, a review of the framework concerning ad hoc prohibited commercial practices could be considered, so that targeted online advertising without lawful prerequisites is deemed per se illegal. In any case, the primary focus of supervisory and regulatory authorities should be on EU and international fora, where their active participation and the development of synergies with other countries can contribute to establishing unified rules for online advertising, with respect to user rights.

ii. Consent Mechanisms and Exercising Rights

The research findings clearly indicate limited awareness among internet users regarding how online advertising operates and the risks involved. Therefore, raising awareness among users about online advertising and micro-targeting is of crucial importance. The research team believes that an informed user can more effectively assert their rights both as a data subject and as a consumer.

Indicative Bibliography

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of retailing*, 91(1), 34-49.

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management*, 49(7), 1089-1110.

Bulchand-Gidumal, J., William Secin, E., O'Connor, P., & Buhalis, D. (2023). Artificial intelligence's impact on hospitality and tourism marketing: exploring key themes and addressing challenges. *Current Issues in Tourism*, 1-18.

D'Amico, Alessia Sophia and Pelekis, Dionysios and Santos, Cristiana and Duivenvoorde, Bram, Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law (March 28, 2024). Utrecht University School of Law Research Paper Forthcoming

Galli, Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD. In: Ebers, M., Cantero Gamito, M. (eds) *Algorithmic Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law*, vol 1. Springer (2021)

Geradin, D., & Katsifis, D. (2020). Taking a dive into Google's Chrome cookie ban.

Geradin, Damien and Katsifis, Dimitrios and Karanikioti, Theano, GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech (May 11, 2020). TILEC Discussion Paper No. 2020-012

Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1-18).

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, 95, 295-306. (Impact factor 2023: 8,958, AJG List 2021: 2)

Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, 36(4), 632-658. AJG:3 in Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of advertising*, 41(1), 59-76.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing*, 55(1), 16-30.

Helberger, N., Borgesius, F. Z., & Reyna, A. (2017). The perfect match? A closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review*, 54(5).

Jabłonowska, 'Consumer Protection in the Age of Data-Driven Behaviour Modification' (2022) *EuCML*, 67 Jarovsky, L., Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness (March 1, 2022)

Laux, J., Wachter, S., & Mittelstadt, B. (2021). Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review*, 58(3).

Margaritis, E. Online Behavioral Advertising as an Aggressive Commercial Practice *Journal of European Consumer and Market Law*, Volume 12, Issue 6 (2023) pp. 243

Ryan, J., & Santos, C. (2022). An Unending Data Breach Immune to Audit? Can the TCF and RTB Be Reconciled with the GDPR?. Can the TCF and RTB Be Reconciled with the GDPR.

Strycharz, J., & Duivenvoorde, B. B. (2021). The exploitation of vulnerability through personalised marketing communication: Are consumers protected?. *Internet policy review*, 10(4), 1-27.

Trzaskowski, Jan, Your Privacy Is Important to Us! – Restoring Human Dignity in Data Driven Marketing (December 6, 2021). Copenhagen Business School, CBS LAW Research Paper No. 21-10, Ex Tuto Publishing

V. Karkatzounis, E. Margaritis, Contract or consent for online advertising? A meta dilemma in the Irish DPC decision on Meta, ΔiMEE, 2/2023

V. Karkatzounis, L. Mitrou, A. Vorras, Regulating AdTech: Chasing Chimeras or the Art of the Possible?, Proportionality in EU Digital Law - Balancing Conflicting Rights and Interests, Bloomsbury Publishing

Van Ooijen, I., Segijn, C. M., & Oprea, S. J. (2022). Privacy cynicism and its role in privacy decision-making. Communication Research, 00936502211060984.

Veale M, Zuiderveen Borgesius F. Adtech and Real-Time Bidding under European Data Protection Law. German Law Journal. 2022;23(2):226-256

Wachter, Sandra, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising (May 15, 2019). Berkeley Technology Law Journal, Vol. 35, No. 2, 2020

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision support systems, 51(1), 42-52. (Impact Factor 2023: 6,969)

Zardiashvili A., Sears A. M., Targeted Advertising and Consumer Protection Law in the EU (2022)

Zuiderveen Borgesius, F. J. (2015). Personal data processing for behavioural targeting: which legal basis? International Data Privacy Law, 5(3), 163-176.

Zuiderveen Borgesius, F. (2013). Consent to Behavioural Targeting in European Law What are the Policy Implications of Insights from Behavioural Economics? Amsterdam Law School Research Paper, (2013-43).