Power and dignity: the ends of online behavioral advertising in the European Union

Zardiashvili, A.

CHAPTER 6. BOUNDARIES OF CONSUMER MANIPULATION VIA OBA

Consumer manipulation via OBA poses various potential harms and systemic threats with varying severity. Although these harms are increasingly recognized, many of the manipulative practices seem to continue to proliferate in the online environment.[894] For example, the OBA infrastructures that facilitate third-party tracking have filled the online environment with manipulative (and coercive) cookie banners that are harmful but remain a standard industry practice.[895] This creates uncertainty as to precisely what the legal boundaries of consumer manipulation via OBA are.[896] With this in mind, this chapter answers the fifth sub-question of the thesis:

SQ5: what are the legal boundaries of consumer manipulation via OBA in the EU?

Section 6.1 provides an overview of the EU legal framework for the OBA. It particularly describes EU consumer protection, data protection, competition law, and legislation within the digital single market strategy, emphasizing platform regulation. Section 6.2 addresses prohibited advertising practices. Section 6.3 elaborates on legal grounds for allowed OBA practices. Section 6.4 considers rules requiring transparency, and risk mitigation. Section 6.5 concludes the chapter and answers the SQ5.

---

[894] *See e.g.,* for harms European Commission Study Recent Digital Advertising Developments, *supra* note 36. *See generally* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53.

[895] *See* Morel et al., *supra* note 546.

[896] *See* Johnny Ryan, *supra* note 55.

6.1. The EU Legal Framework for OBA

The European Union (EU) has been established with various aspirational goals. "Internal market", a single market free of obstacles where people, goods, and capital could move freely, was thought to achieve these objectives. Therefore, most EU legislation seeks to harmonize the legislation of different member states regarding key areas for the Europe-wide single market. This thesis focuses on the areas of law that create such a single market, and that intend to safeguard consumer autonomy by setting boundaries for the targeting methods in advertising practices. Such areas of law include consumer protection (section 6.1.1), personal data protection (section 6.1.2), competition law (section 6.1.3), and a variety of legal acts and proposals that specifically address the "digital" single market (section 6.1.4).

This thesis does not analyze intellectual property law, including copyright and trademarks, that typically safeguard business interests instead of consumer autonomy. This thesis also does not comprehensively analyze law focusing on media pluralism, non-discrimination, and the environment. Such a scope is justified due to the focus of this thesis on consumer manipulation and consumer autonomy. As OBA is primarily a commercial practice, the thesis scoped its analyses in a commercial context, excluding analysis of rules regarding political advertising.

6.1.1. EU Consumer Protection Law

As with all advertisements, OBA is a commercial practice typically directed to consumers.[897] Consumer manipulation is a form of consumer exploitation, and its harms fall within the scope of consumer protection rules, which is one of the EU policy's critical tasks and competencies.[898] Consumer protection is a particular area of private law that recognizes the asymmetrical relationship between businesses and consumers and grants certain protections to consumers regarded as the weaker party in such commercial dealings.[899] In the EU legal framework, rules protecting

[897] *See generally* Zard and Sears, *supra* note 1. Note that ads can also be directed to recipients of services that are businesses.

[898] The EU consumer protection foundation was laid out in Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a Consumer Protection and Information Policy, 1975 O.J. (C 92) 1, 1–16. This resolution was inspired by the U.S. President Kennedy's formulation of consumer rights. *See* John F. Kennedy, Special Message to the Congress on Protecting the Consumer Interest (March 15, 1962). According to Article 12 TFEU "Consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities." *See* TFEU, *supra* note 59, art. 12. According to Article 169(1) TFEU, "In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organize themselves in order to safeguard their interests." *Id.* art. 169(1).

[899] *See* V. Mak, *The Consumer in European Regulatory Private Law. A Functional Perspective on Responsibility, Protection and Empowerment*, *in* THE IMAGE(S) OF THE CONSUMER IN EU LAW: LEGISLATION, FREE MOVEMENT AND COMPETITION LAW 381 (Dorota Leczykiewicz & Stephen Weatherill eds., 2016).

consumers' interests, including in the context of OBA, are laid down in various pieces of consumer protection legislation.[900] Particularly relevant are the Consumer Rights Directive (CRD),[901] the Unfair Contract Terms Directive (UCTD),[902] and the Unfair Commercial Practices Directive (UCPD).[903] The Modernisation Directive (MD) was intended to update these consumer protection rules in light of digital services.[904] This legislative framework aims to ensure consumer autonomy in a commercial relationship by safeguarding them against harms to their economic interests, as well as promoting their psychological and physical well-being.[905] It intends to achieve these goals by empowering consumers with information ("information paradigm")[906] and protecting them from otherwise unfair contractual terms and practices ("unfairness paradigm").[907]

The information paradigm permeates all consumer protection rules, which are based on the assumption that if consumers have enough information, they will exercise their autonomy by making informed decisions according to their individual goals, values, and preferences.[908] Such an understanding of a consumer as a "reasonably well-informed, and reasonably observant and circumspect" is at the core of consumer protection law, often formulated as an "average consumer" benchmark.[909] In other words, such a benchmark assumes that an average consumer will analyze the information provided and act accordingly.[910] The CRD, in

[900] There are other pieces of legislation that contain consumer protection rules relevant for OBA, but that are not primarily regarded as consumer protection legislation. *See* Christoph Busch & Vanessa Mak, *Putting the Digital Services Act in Context*, 10 J. EUR. CONSUM. MARK. LAW (2021).

[901] Directive (EU) 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council O.J. 2011 (L 304) [hereinafter Consumer Rights Directive].

[902] Directive (EEC) 93/13 of the Council of 5 April 1993 on unfair terms in consumer contracts, O.J. 1993 (L 95) 29 [hereafter Unfair Contract Terms Directive].

[903] Unfair Commercial Practices Directive, *supra* note 42.

[904] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, O.J. 2019 (L 328) 7 [hereinafter Modernisation Directive].

[905] *See* TFEU, *supra* note 59*,* art. 169(1).

[906] *See* TRZASKOWSKI, *supra* note 421, at 270.

[907] *See* Helberger, Zuiderveen Borgesius & Reyna, *supra* note 41, at 9.

[908] *See* TRZASKOWSKI, *supra* note 41 at 181.

[909] *See* Case C-210/96, *Gut Springenheide & Tusky v. Oberkreisdirektor des Kreises Steinfurt*, 16 July 1998, ECLI:EU:C:1998:369., I–4691. *See also* Case C-371/20, *Peek & Cloppenburg*, 2 September 2021, ECLI:EU:C:2021:674., 21, 41. ("[E]xplaining that the purposes of the provisions of the Unfair Commercial Practices Directive are to indicate the existence of commercial influence so that the influence is "understood as such by the consumer").

[910] *See* Case C-210/96, *Tusky*, *supra* note 911 at I–4691. *see also* Case C-371/20, *Peek & Cloppenburg*, *supra* note 911, at 21, 41.

particular, includes extensive information requirements when businesses contract with consumers.[911] This includes "distance contracts" for providing digital services.[912] When such services are provided, the CRD requires service providers (including platform providers and other publishers) to disclose information about, *inter alia*, the main characteristics of the service,[913] their identity and contact details,[914] the price,[915] and functionality,[916] which can include the fact that consumers will be tracked;[917] and that prices are personalized.[918] Section 6.3.1.3 discusses to what extent these requirements apply in the context of the OBA industry when the counter-performance of contracts is personal data instead of monetary payment.

The unfairness paradigm in the UCTD ensures the protection of consumers from contract terms that are drafted by businesses in advance, which can be detrimental to consumer interests and which consumers are incapable of changing because of information and (bargaining) power asymmetries.[919] Such terms may be present in standard-form contracts, used for most if not all, contracts for digital services and content.[920] For example, a contract clause allowing businesses to change contract terms unilaterally, without a consumer's consent, is typically considered unfair.[921] Moreover, the UCTD discourages ambiguity by prescribing that unfair terms must be interpreted favorably to the consumer – *in dubio contra stipulatorem* principle.[922] Unfair terms cannot be binding for consumers and can render contracts null and void.[923] Nevertheless, the ultimate unfairness test of

[911] Consumer Rights Directive, *supra* note 903, art. 6.

[912] *Id.,* art 2(7). ("'distance contract' means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;")

[913] *Id.,* art 6(1)(a).

[914] *Id.* art. 6(1)(b)–(d).

[915] *Id.* art. 6(1)(e).

[916] *Id.* art. 6(1)(r).

[917] *Id.* rec. 19.

[918] Consumer Rights Directive, *supra* note 903, art. 6(1)(e).

[919] EUROPEAN PARLIAMENT, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS DIRECTORATE-GENERAL FOR INTERNAL POLICIES, *Study on the Update the Unfair Contract Terms Directive for Digital Services*, 10 (2021).

[920] John J. A. Burke, *Contract as Commodity: A Nonfiction Approach*, 24 SETON HALL LEGIS. J. 285, 290 (2000).("[I]n an advanced economy the standard form contract accounts for more than 99 percent of all contracts used in commercial and consumer transactions for the transfer of goods, services and software.").

[921] Unfair Contract Terms Directive, *supra* note 904, annex I, art. 1(j).

[922] *Id.* at 5.

[923] *Id.* at 6.

business-to-consumer commercial practices, such as OBA, is the UCPD, the safety net for safeguarding consumer autonomy, including against manipulation.[924]

The UCPD includes three tiers of prohibitions of "unfair practices". Firstly, Article 5(2) of the UCPD prescribes a general prohibition of unfairness in commercial practices, laying out two cumulative requirements for regarding a practice unfair: "(a) it is contrary to the requirements of *professional diligence*, and (b) it materially distorts or is likely to *materially distort* the economic behavior. . . of the average consumer."[925] Secondly, the UCPD provides more specific provisions by which practices are prohibited, in particular, two more specific categories of unfair practices: "misleading" (Articles 6-7 UCPD) and "aggressive" (Articles 8-9 UCPD).[926] When determining whether a practice is misleading or aggressive, it must be assessed whether it causes or is likely to cause the "average consumer" to make a transactional decision that the consumer would not have otherwise made.[927] Thirdly, the UCPD contains a blacklist in Annex I, where thirty-five practices are explicitly prohibited because they are misleading or aggressive.[928]

To evaluate whether a practice is unfair and therefore prohibited by the UCPD, one must examine the practice in three steps, from the most specific to the most general prohibition. First, it needs to be established whether the practice is listed in Annex I as one of the blacklisted practices.[929] In such a case, no further consideration is necessary, and the practice is prohibited. Second, if the practice is not listed in Annex I, it must be assessed whether the practice is either misleading (through actions[930] or omissions[931]) or aggressive,[932] including whether it exerts undue influence.[933] In case such misleading or aggressive practices have or are likely to have an economic effect as described above, they can be found unfair and deemed prohibited. Third, as a last resort, when the first two situations don't apply, the most general provision of the UCPD prohibits practices that are *otherwise*

[924] *See* Unfair Commercial Practices Directive, *supra* note 42, arts. 3(1), 5(1), 1. (for business to consumer relationships, prohibition of unfair practices, and economic interests, respectively).

[925] *Id.* at art 5(2)(a)-(b). (emphasis added). Article 5(2)(b) states in full that "it 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." *Id.* art. 5(2)(b).

[926] *See Id*. arts. 6–9.

[927] *See* TRZASKOWSKI, *supra* note 41, at 181.

[928] *See* Unfair Commercial Practices Directive, *supra* note 42, art. 5, annex I.

[929] *Id*. annex I.

[930] *Id*. art. 6.

[931] *Id*. art. 7.

[932] *Id*. art. 8.

[933] *Id*. art. 9.

contrary to the requirements of professional diligence.[934] For example, this can be the case if the practice violates a code of conduct applicable to the industry.

The framework of influence developed in this thesis matches the UCPD's framework of dividing "unfair" practices into misleading and aggressive. In particular, misleading actions and omissions refer to situations of *deception* when some aspect of influence is hidden from the consumer. Aggressive practices typically refer to situations of undue influence through *pressure*. OBA practices tailored to exploit consumer vulnerabilities can be regarded as aggressive under the UCPD. Note that whether the aggressive practice is a manipulative or coercive attempt depends on whether all essential aspects of influence are clear for the consumer.

One hesitation with applying consumer protection rules to OBA has been the focus of this field of law on consumers' economic behavior and interests.[935] Regardless of such a focus, most commentators believe that consumer protection rules can be expanded to safeguard against other fundamental rights and interests.[936] Therefore, there is growing consensus amongst judiciary, policymakers, and academia that consumer protection law applies in the context of OBA in its entirety, including in two separate stages identified in this thesis.[937] Firstly, during the *contracting* stage – when consumers agree to exchange their attention, time, and data for receiving digital services, and secondly, during the *advertising* stage – when they are exposed to advertisements.[938] The extent to which this framework is able to safeguard against the full range of consumer manipulation harms of OBA is still the subject of debate.[939]

The key question is regarding the image of the consumer in the online environment and whether a consumer is thought of as vulnerable. There has been an academic consensus on "digital asymmetry" between digital service providers and consumers, and therefore, the a need for consumer protection law to consider the online consumer as more than ordinarily vulnerable.[940] However, there is no case law yet that firmly establishes such an image of the consumer. In case the

[934] Otherwise, because misleading or aggressive practices are per se against professional diligence, therefore all blacklisted practices as well. *See id.* art. 5.

[935] *See generally* Helberger, Zuiderveen Borgesius, and Reyna, *supra* note 41.

[936] *See* Thomas Wilhelmsson & Chris Willett, *Unfair Terms and Standard Form Contracts*, *in* HANDBOOK OF RESEARCH ON INTERNATIONAL CONSUMER LAW 139, 159–60 (Geraint Howells et al. eds., 2d ed. 2018).

[937] *See generally* Zard and Sears, *supra* note 1.

[938] *See* Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services O.J. (L 136) 1 [hereinafter Digital Content Directive].

[939] *See e.g.,* Hacker, *supra* note 54.

[940] Vanessa Mak, *A Primavera for European Consumer Law: Re-Birth of the Consumer Image in the Light of Digitalisation and Sustainability*, 11 J. EUR. CONSUM. MARK. L. 77 (2022).

vulnerability of the online consumer is acknowledged, the UCPD prohibits all consumer manipulation via OBA, and therefore, complete protection of the consumer manipulation harms of OBA. CJEU is currently considering Case C-646/22 *Compass Banca* to address the question of whether the (not necessarily digital) average consumer is rational or one with bounded rationality, or as this thesis refers to as, "ordinarily vulnerable".[941] Recognition of the baseline vulnerability of all consumers would be a significant step in reforming consumer protection law enforcement. Nevertheless, separate court consideration for the increased vulnerability of online consumers may be needed for effective enforcement.

In other words, this thesis holds that while consumer protection law provides substantive safeguards against consumer manipulation via OBA, enforcing this practice may be challenging and require the bravery of the enforcers until there is an explicit recognition of consumer online vulnerability by the CJEU. Apart from a consumer benchmark, enforcing consumer protection rules can be a challenge concerning OBA for other reasons. Consumer protection authorities (CPAs) enforce consumer protection rules within the Member States. Consumers typically bring claims to CPAs or courts themselves about the violations. Representative Actions Directive (RAD) allows collective legal action claims by entities representing consumers. RAD entered into force on 2 May 2023, which may significantly affect the enforcement of consumer protection rules in the context of OBA.[942]

Most importantly, the UCPD is a consumer complaint-based tool that is well-placed in case the consumer is facing coercive exploitation by the business but may be less effective when the consumer faces manipulative and, thus, hidden, exploitation.[943] Due to the challenges of enforcement associated with consumer protection law, consumer manipulation harms of OBA have historically been primarily discussed in the context of the personal data protection framework. While theoretically, there is no hierarchy within the fundamental rights, in practice, "freedoms" listed in Title II, such as the right to personal data protection, are historically more straightforward to enforce as fundamental rights than the rights listed in Title IV, such as the right to consumer protection, which are sometimes seen as aspirational.[944]

---

[941] *Case C-646/22*, Compas Banca Request*, supra* note 434.

[942] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance), 409 OJ L (2020).

[943] CPDPConferences, *The End of Online Behavioral Advertising*, YOUTUBE (2023), https://www.youtube.com/watch?v=FwMz7OLoOXI (last visited Jul 20, 2023).

[944] *See* Helena U.Vrabec, *Uncontrollable: Data Subject Rights and the Data-Driven Economy* (Leiden University, Dissertation, 2019). *See e.g.,* Case C-470/12, Pohotovosť v. Mheleniroslav Vašuta, 27 February 2014, ECLI:EU:C:2014:101. ("In that regard, Article 38 of the Charter provides that European Union policies must ensure a high level of consumer protection. That requirement also

6.1.2. EU Personal Data Protection Law

Personal data protection legislation has been the hallmark of the EU response to prevent and mitigate harms stemming from the advance of information technologies that process personal data.[945] The CFREU that included personal data protection as an individual fundamental right was proclaimed in 2000, shortly before Alphabet adopted OBA as a business model.[946] Article 8 of the CFREU reiterates the EU approach to the processing of personal data, which, in essence, is only allowed in case there is sufficient legal ground provided by law, such as, for example, the consent of the person involved.[947] The CFREU went into force in 2009, shortly after Facebook launched its advertising platform, including the controversial advertising *Beacon* that covertly tracked users over the Internet.[948] The rise of social networks and OBA as the backbone of the online environment have largely triggered a call to update personal data protection rules, resulting in the adoption of the General Data Protection Regulation (GDPR), which entered into force on May 25, 2018.[949]

The GDPR applies to OBA to the extent that it involves processing personal data, broadly defined as "any information relating to an identified or identifiable natural individual ('data subject')."[950] This definition is of paramount importance and has attracted controversy as to what extent behavioral data processed for OBA

applies to the implementation of Directive 93/13 [on consumer rights]. However, since Directive 93/13 does not expressly provide for a right for consumer protection associations to intervene in individual disputes involving consumers, Article 38 of the Charter cannot, by itself, impose an interpretation of that directive which would encompass such a right.") *See also* Monika Jagielska & Mariusz Jagielski, *Are Consumer Rights Human Rights?*, *in* EUROPEAN CONSUMER PROTECTION: THEORY AND PRACTICE 336 (James Devenney & Mel Kenny eds., 2012).

[945] JIAHONG CHEN, REGULATING ONLINE BEHAVIOURAL ADVERTISING THROUGH DATA PROTECTION LAW 93 (2021).

[946] *See* for detailed overview about emeregance of personal data protection as the fundamental right in Gloria González Fuster, *EU Fundamental Rights and Personal Data Protection*, *in* THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 163 (Gloria González Fuster ed., 2014).

[947] CFREU, *supra* note 46, art. 8. *See also* CHEN, *supra* note 947 at 92.

[948] *See for* Facebook Beacon in Betsy Schiffman, *Facebook Is Always Watching You*, WIRED, Dec. 4, 2007, https://www.wired.com/2007/12/facebooks-is-al/ (last visited Apr 20, 2023).

[949] In the memorandum IP/10/63 from January 28, 2010, Commission calls for reform of the personal data protection rules. It starts by declaring that "Our privacy faces new challenges: behavioural advertising can use your internet history to better market products; social networking sites used by 41.7 million Europeans allow personal information like photos t be seen by others". European Commission Press Release IP/10/63, The Commission, *supra* note 44. It also points to the Phorm's predatory OBA in the UK as the concerning practice. Viviane Reading, the Commissioner, has also addressed this in her speech. Viviane Reding Member of the European Commission responsible for Information Society and Media Privacy: the challenges ahead for the European Union Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels, SPEECH/ 10/16 (Jan. 28, 2010), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_10_16.

[950] General Data Protection Regulation, *supra* note 44, art. 4.

can be considered personal data.[951] By the time the GDPR entered into force in 2018, there was consensus that OBA constitutes personal data processing because it enables singling out a particular individual, even without having data connected to a person's name.[952] Applying the GDPR to OBA means that OBA is only allowed if there is a legal ground for processing (Article 6 GDPR) and such processing is in accordance with the data protection principles (Article 5 GDPR).[953] Three legal grounds that digital service providers have relied on for OBA include (a) the data subject's consent, (b) the necessity for the performance of a contract with a data subject, and (f) legitimate interests, for example, the economic interest of the OBA industry in providing advertising.[954] Under the GDPR, such legitimate interest can be a lawful ground only after evaluating that it does not override the human rights interests of data subjects, requiring a balancing exercise.[955]

The GDPR's consent requirement (further discussed in section 6.3.1.1) as a legal ground for processing is often confused with consent in cookie banners that have permeated the online environment and that have emerged for complying with the ePrivacy Directive, another legal instrument in the EU personal data and privacy protection framework.[956] The ePrivacy Directive, historically protecting privacy in the electronic communications sector, applies to OBA to the extent it deploys tracking technologies, such as cookies, that store information on or gain access to information already stored in a consumer's devices (e.g., connected devices).[957] It applies regardless of whether the consumer's information is classified as personal

[951] CHEN, *supra* note 947 at 94.

[952] Frederik J. Zuiderveen Borgesius, *Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, 32 COMPUT. LAW SECUR. REV. 256 (2016). *See* General Data Protection Regulation, *supra* note 44, rec. 30. ("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, in particular 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.")

[953] General Data Protection Regulation, *supra* note 44, art. 5; *Id.* art. 6.

[954] General Data Protection Regulation, *supra* note 44, art 6.

[955] *Id.,* art. 6 (f).

[956] ePrivacy Directive, *supra* note 43. The consent for the placement of cookies is different from the legal grounds for processing personal data. For example, the ground for processing of personal data can be legitimate interest (e.g., marketing), but if such processing requires placement of tracking technologies, such placement still requires consent. The effect in this case is that publishers can provide their services only if consumers accept the cookies. Same is not true if the legal ground for processing is consent, in which case refusal to data processing cannot result in publisher suspending their services or content (otherwise it would not be freely given).

[957] *Id.* at 5(3).

data under the GDPR.[958] The ePrivacy Directive requires consent for deploying such technologies for advertising purposes, and the OBA-funded online environment has been filled with cookie banners requiring consumers to accept such cookies on many of the websites they visit.[959]

In order to avoid the proliferation of cookie banners in the online environment, the EU proposed the ePrivacy Regulation in 2017.[960] The proposal included the requirement to centralize tracking decisions in browser settings that would allow consumers to choose how they wanted to be tracked over the Internet.[961] Such a rule allowed consumers to choose not to be tracked over the Internet and threatened the OBA industry with heavy financial losses. This regulation has been wholly stalled since the end of 2021.[962] This has given the OBA industry the time to continue exponential wealth-creation and to come up with a privacy-preserving versions of OBA while at the same time proliferating cookie banners in the online environment, most of which are manipulative.[963]

The EU privacy and personal data protection regime goes beyond the requirements for data collection. The GDPR further requires OBA to meet the data protection principles when processing personal data.[964] In other words, in order for OBA to be considered a legitimate practice, it not only has to be lawful (based on one of the legal grounds) but also *fair* and *transparent* (meet data protection principles of "lawfulness, fairness, and transparency").[965] The principles of fairness and transparency are closely related to the data subject's autonomy, similar to consumer protection law unfairness and information paradigms. However, the personal data protection regime provides stronger protections: the GDPR enables autonomy by *taking proactive measures* for ensuring that data subjects understand how their data is used (the "transparency paradigm") and that personal data is not used in a way that undermines the data subject's interests, for example, by having a discriminatory effect, or by unfair balancing of interests (the "fairness

[958] *Id.* at 2(d). ("'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.")

[959] *Id.* at 5(1).

[960] Proposal for ePrivacy Regulation, *supra* note 43.

[961] *Id.* recs. 23-25.

[962] Proposal for a regulation on privacy and electronic communications, Legislative Train Schedule, EUROPEAN PARLIAMENT (2023), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform (last visited Dec 21, 2023).

[963] Most prominent project has been Google's Privacy Sandbox that has intended to change OBA with technology that does not rely on cookies. Its use has continuously postponed, and now is considered to come into play in 2004 Chavez, *supra* note 245; The Privacy Sandbox: Technology for a More Private Web, PRIVACY SANDBOX, https://privacysandbox.com/ (last visited Apr 23, 2023).

[964] Article 5 of the GDPR includes six data protection principles: (a)"lawfulness, fairness and transparency", (b)"purpose limitation", (c)"data minimization", (d)"accuracy", (e)"storage limitation", (f)"integrity and confidentiality". *See* General Data Protection Regulation, *supra* note 44, art. 5.

[965] *Id.*, art. 5.

paradigm").[966] Central here is that the GDPR shifts the burden of proof towards the business to ensure that in their attempt to ensure transparency, businesses do not merely disseminate information but ensure that consumers understand the information.[967]

The GDPR offers increased protections for processing personal data that can be particularly sensitive, arguably due to increased risk of harm.[968] Such "special categories" of personal data include information "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[969] Processing such data for OBA is considered unfair and prohibited (section 6.1.4). However, the GDPR's dual categorization of data into special and non-special categories is widely criticized: the lines between such data are blurred, making it difficult to distinguish one from the other. Also, the issue is the potential for harm that can often come from non-special categories of data.[970]

The GDPR introduces a variety of data subjects' rights, such as the right to access, erase, or rectify one's personal data, withdraw consent, and object to processing.[971] A "data controller," or the businesses, can decide how to use personal data and whether to conduct a "data protection impact assessment" (DPIA) in cases where there is a heightened risk of harming interests protected by the interests of the fundamental rights.[972] The GDPR introduces a variety of additional safeguards, such as a requirement for data controllers to appoint data protection officers (DPOs)[973] that report to data protection authorities (DPAs)[974] and establishes the role of a European Data Protection Supervisor (EDPS) that acts as the data protection authority of the EU institutions.[975] DPAs of all member states also create the European Data Protection Board (EDPB) that provides guidance and interpretation of the GDPR and promotes its consistent application within the EU by resolving disputes and issuing guidelines and binding decisions. The EDPB was formed on an

[966] Gianclaudio Malgieri, *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation*, *in* PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 154 (2020).

[967] *See* TRZASKOWSKI, *supra* note 41, at 181–183.

[968] General Data Protection Regulation, *supra* note 44, art. 9.

[969] *Id.*

[970] *See generally* Solove, *supra* note 631. *See also* Paul Quinn & Gianclaudio Malgieri, *The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework – CORRIGENDUM*, 23 GER. LAW J. 688 (2022).

[971] General Data Protection Regulation, *supra* note 44,arts. 12-23.

[972] *Id.* art. 5, 35.

[973] *Id.* arts. 37-40.

[974] *Id.* arts. 51-54.

[975] *Id.* arts 57-59.

existing body, the *Article 29 Working Party* (A29WP), that interpreted the Data Protection Directive before the GDPR. The GDPR also introduced significant sanctions for violations of data protection rules. Depending on the violation, the maximum can be €10-20 million or up to 2-4% of the global annual revenue of a company, whichever is higher.[976]

When it comes to OBA, many commentators thought of OBA as fundamentally inconsistent with the personal data protection rules due to its large-scale processing of personal data over the Internet.[977] Nevertheless, the OBA continues to create wealth for the industry – it has contributed to generating more than $1.3 trillion in revenue for Alphabet in two decades and more than $ 0.5 trillion for Meta in a decade.[978] Market studies find that OBA allows companies with unparalleled access to consumer data to earn excess profits that are way above the fair benchmarks for their shareholders.[979] Section 6.1.3 illustrates to what extent the EU competition law applies to OBA.

6.1.3. EU Competition Law

Ensuring competition in the "single market" is another central task of the European Union.[980] The EU competition policy aims to support the creation and preservation of the single market and to ensure the efficient allocation of resources with an ultimate aim to promote consumer welfare (section 5.1.2).[981] EU competition law is a tool for meeting such policy objectives by ensuring that

[976] *Id.* arts. 83–89.

[977] Scott Ikeda, *Report on RTB: Adtech "Biggest Data Breach Ever Recorded," Online Behavior More Exposed in Countries Without Privacy Regulations*, CPO MAGAZINE, May 24, 2022, https://www.cpomagazine.com/data-privacy/report-on-rtb-adtech-biggest-data-breach-ever-recorded-online-behavior-more-exposed-in-countries-without-privacy-regulations/ (last visited Oct 13, 2023).

[978] *See Google revenue 2002-2022*, STATISTA, https://www.statista.com/statistics/266206/googles-annual-global-revenue/ (last visited Apr 23, 2023). *See Meta: annual revenue and net income 2022*, STATISTA (2023), https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/ (last visited Apr 23, 2023).

[979] *See* European Commission Study Recent Digital Advertising Developments, *supra* note 36.

[980] Article 3 of the Treaty of Rome establishing the European Economic Community (EEC) predecessor of the EU stated that the activities of the EEC should include: "a system ensuring that competition in the internal market is not distorted." Treaty of Rome Establishing the European Economic Community, Mar. 25, 1957, 1957, art. 3(f). *See also* Consolidated Version of the Treaty establishing the European Community, Dec. 24, 2002, O.J. (C 325), art. 3(g). Lisbon Treaty took out this provision from the treaty text, but affirmed the same in the protocol that has the same legal weight. *See* TEU, *supra* note 60, Prot No. 27.

[981] A lot has been written about the goals of the EU competition policy. Historically, market integration – the creation of the EU single market – was seen as an ultimate goal, but consumer welfare and allocative efficiency goals have developed in parallel. Recently, Commission has formulated the objectives to conceptualize market integration and competition to serve a common goal – consumer welfare. *See* JONES AND SUFRIN, *supra* note 645 at 43.

businesses do not use their market power to distort competition.[982] In particular, Article 101 of the Treaty of the Functioning of the EU (TFEU) prohibits businesses from engaging in anti-competitive behavior, and Article 102 prohibits them from abusing their "dominant position within the internal market".[983] In the EU, these rules are called "antitrust".[984] The EU Merger Regulation 139/2004 (EUMR) provides rules for reviewing mergers and acquisitions to ensure they do not distort competition within the common market.[985] The European Commission is the key enforcer and decision-maker of the antitrust and merger rules in the European Union through its Director-General for Competition (DG Comp).[986] However, it closely cooperates with the national competition authorities (CAs), who are responsible for applying and enforcing the EU competition law in their respective jurisdictions and who join DG Comp in the European Competition Network (ECN) .[987]

The *Google/DoubleClick* decision of the European Commission in 2008 is a landmark case that set the stage for EU competition law in the context of online advertising.[988] It is particularly important because of the way it defines online advertising markets. In this decision, the European Commission separates *offline* and *online* advertising markets,[989] *search* and *display* advertising markets,[990] and closed (on-platform) and open (AdTech) markets.[991] At the time, DoubleClick was a globally leading *ad server* for publishers and advertisers and was about to launch an *ad exchange* – an intermediary in the online advertising ecosystem (Chapter 2). The European Commission recognized the possibility that a merger would considerably

[982] *Id.* at 1.

[983] TFEU, *supra* note 59, arts. 101-102. Note that, Article 101 prohibits intention as well as an effect of the anticompetitive conduct. ("The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market[…]")

[984] *Antitrust law* is U.S. term for competition law. However, the Commission now uses "antitrust" as a term to denote areas of competition law other than merger control and state aid, that typically encompass anticompetitive agreements and abuse of dominant position under Articles 101-102 of the TFEU.

[985] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) (Text with EEA relevance), 024 OJ L 139 (2004).

[986] JONES AND SUFRIN, *supra* note 645 at 89. In plain terms, the Commission acts as the prosecutor and the judge in competition law cases. The cases can be further appealed in the CJEU.

[987] *Id.* at 93.

[988] Commission Decision C(2008) 927 in Case No Comp/M4731 - Google/DoubleClick 2008.

[989] *Id.* 44–46.

[990] *Id.* at 48–56.

[991] *Id.* at 20–23. It does recognize targeting techniques (behavioral/contextual) as the way to categorize the market but instead chooses to focus on delivery channels. Therefore two large markets of search and display; with four sub-markets on-platforms (closed) search advertising market, open search intermediation market, on-platforms (closed) display advertising market, open display intermediation market. Further in this case, Commission recognized separate market for *ad servers* that DoubleClick operated in. The case addresses ad server and open display intermediation markets primarily.

increase Google's (now part of Alphabet) power in the open display advertising market but dismissed its relevance, doubting that Alphabet could leverage DoubleClick data for advertising and intermediation.[992] Moreover, the European Commission completely refrained from evaluating concerns about consumers' privacy and autonomy arising from the merger.[993] It even described Google's OBA practices to potentially compete with "deep packet inspection" methods, which from the lense of consumer privacy, even then, were fundamentally illegal.[994]

Contrary to the European Commission's predictions, the DoubleClick acquisition has cemented Google's dominance in online advertising, including in the AdTech or open exchange display advertising market (section 2.3.3).[995] Following the *Google/DoubleClick* decision and in response to the meteoric rise of Google's market power, the European Commission has concluded three large-scale antitrust investigations and has fined Google for abusing its dominance by "self-preferencing", i.e., giving an advantage to its own services over competitors in cases of *Google Shopping* (€2.4 billion some),[996] *Google Android* (€4.34 billion fine),[997] and *Google AdSense* (€1.49 billion fine).[998] Moreover, French,[999] UK,[1000] and

[992] *Id.* at 230–231, 256. ("If this (ad serving) data allowed DoubleClick to offer a service to its ad intermediation customers that is superior to the service offered by its competitors in the intermediation market which do not have access to this data, advertisers and publishers would inevitably flock to DoubleClick's ad serving and, by extension, to its newly-created ad intermediation service, by virtue of a direct network effect and DoubleClick's bundled offering (ad serving plus ad intermediation) could be very well placed to compete with Google's bundled offering (which would be weaker on behavioural targeting but stronger on search capabilities and established as a successful integrated platform.") The Commission dismissed this potential because it concluded that contractual relationship would not allow the DoubleClick to use the data for this purpose.

[993] *Id.* at 368.

[994] *Id.*

[995] *See Critics pan Google-DoubleClick ruling*, POLITICO (2008), https://www.politico.eu/article/critics-pan-google-doubleclick-ruling/ (last visited Apr 25, 2023). *See also* Jenny Lee, *The Google-DoubleClick Merger: Lessons From the Federal Trade Commission's Limitations on Protecting Privacy*, 25 COMMUN. L. POL'Y 77 (2020).

[996] Commission Decision of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)) C(2017) 4444.

[997] Commission Decesion of 18.7.2018 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (the Treaty) and Article 54 f the EEA Agreement Case At.40099 Google Android (C (2018) 4761.

[998] Commission Decision of 20.3.2019 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (the Treaty) and Article 54 of the EEA Agreement (AT. 40411 - Google Search (AdSense)). In the EU competition law dominance refers to "a position of economic strength enjoyed by an undertaking, which enables it to prevent effective competition being maintained on a relevant market, by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of consumers." Case 85/76, *Hoffmann-La Roche v. Commission*, 13 February 1979, ECLI:EU:C:1979:36.

[999] *See* AUTORITÉ DE LA CONCURRENCE, *Opinion No. 18-A-03 of March 2018 on Data Processing in the Online Advertising Sector*, (2018).

[1000] *See* CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33.

Spanish[1001] competition authorities have conducted online advertising market studies finding that Alphabet dominates all search advertising and open exchange (AdTech) display markets.[1002] Meta's platforms hold a significant market share (40-50%) in the remaining display advertising market.[1003]

These studies illustrate that Alphabet and Meta hold market power mainly due to their access to consumer behavioral data (i.e., "data power").[1004] Accordingly, in June 2021, the European Commission initiated formal proceedings to investigate Alphabet regarding its data-driven advertising practices in the open exchange display market (case is titled *Google AdTech*)[1005] and Meta for potential anti-competitive usage of data for advertising.[1006] On June 14, 2023, regarding the *Google AdTech* case, the European Commission sent a statement of objections to Alphabet regarding suspected violations in the AdTech market.[1007] The European Commission suspected that after acquiring *DoubleClick*, Alphabet dominated all aspects of the open exchange (DSP, SSP, ad exchange) and engaged in anti-competitive behavior by self-preferencing its own services.[1008] The European Commission considers Alphabet's abuse of dominance challenging to remedy by any other means than to divest part of its services, which is the strongest of the remedies available to the competition authority in the EU.[1009] The European Commission investigations are focused on the data power that Alphabet and Meta hold in advertising markets, which directly relates to the ability of these companies to exploit consumer vulnerabilities when relying on these data.

It has been previously argued that consumer exploitation, such as consumer manipulation via OBA, can be regarded as an anti-competitive practice and the abuse of a dominant position by the gatekeepers.[1010] This thesis strongly supports

[1001] *See* CNMC (Spain) Study Competition in Online Advertising, *supra* note 34.

[1002] Elettra Bietti, *Structuring Digital Platform Markets: Antitrust and Utilities' Convergence*, 2024 UNIV. ILL. LAW REV. (2024).

[1003] Damien Geradin & Dimitrios Katsifis, *An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age*, 15 EUR. COMPET. J. 55, 69 (2019).

[1004] *See generally* Davola and Malgieri, *supra* note 35.

[1005] European Commission, *AT.40670 Google - Adtech and Data-Related Practices* (2021). ("The Commission intends to investigate whether Google has violated EU competition rules by favoring, through a broad range of practices, its own online display advertising technology services in the so called "ad tech" supply chain, to the detriment of competing providers of advertising technology services, advertisers and online publishers.") The Commission also closed its proceedings of the 'Jedi Blue' project about the agreement of Meta and Google European Commission, *AT.40774 Google-Facebook (Open Bidding) Agreement*, (2022).

[1006] European Commission, *AT.40684 Facebook Marketplace* (2021).

[1007] European Commission Press Release IP/23/3207, The Commission, *supra* note 47.

[1008] *Id.*

[1009] Remarks by Executive Vice-President Vestager on the Statement of Objections sent to Google over practices in the online advertising technology industry, EUROPEAN COMMISSION (2023), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_3288 (last visited Jul 16, 2023).

[1010] *See* Graef, *supra* note 46.

this argument and frames the issue as a "consumer manipulation market trap" – if gatekeepers are able to exploit the consumers, they are able to earn profit without providing benefits to consumers and engage other digital service providers into competition for consumer exploitation in which gatekeepers have a competitive advantage. Consumer manipulation market trap can lead to excess profits for gatekeepers at the expense of consumers, but also of advertisers and publishers.[1011]

The CAs increasingly recognize such feedback loops.[1012] *Bundeskartellamt,* the German Federal Cartel Office, has led the EU competition enforcement for gatekeepers by recognizing that platform consumer exploitation (breach of privacy rules) can also abuse dominance.[1013] *Bundeskartellamt* found that Meta used its market power to extract consumers' consent for processing their personal data for OBA purposes by combining such data between its services (i.e., Whatsapp, Instagram, and Facebook).[1014] Meta has challenged this case with the CJEU, arguing that the competition authority cannot consider data protection rules when weighing interests under antitrust investigation.[1015] On July 4, 2023, the CJEU issued a judgment in the *Meta v. Bundeskartellamt* case that justified the competition authority in evaluating data protection rules in its antitrust investigation.[1016] This is a landmark decision that can be considered a significant step towards adopting a holistic approach to resolving OBA harms.[1017]

Bringing the discussion on consumer autonomy and fairness of personal data processing within competition law is a significant change in practice. Scholars increasingly suggest that competition authorities integrate consumer autonomy into

[1011] CNMC (Spain) Study Competition in Online Advertising, *supra* note 34 at 145. *See* Davola and Malgieri, *supra* note 35.

[1012] *See* CNMC (Spain) Study Competition in Online Advertising, *supra* note 34 at 144–146. *See also See e.g.,* Nicholas Economides & Ioannis Lianos, *Privacy and Antitrust in Digital Platforms*, (2020), https://papers.ssrn.com/abstract=3755327 (last visited Apr 26, 2023).

[1013] Bundeskartellamt [BKartA] Case VI-Kart 1/19 (V), Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (Facebook), 26 August 2019, ECLI:DE:OLGD:2019:0826.VIKART1.19V.0A (Ger.).

[1014] *Id.*

[1015] Case C-252/21, *Meta v. Bundeskartellamt*, ECLI:EU:C:2023:537.

[1016] *Id.*

[1017] *See* Natasha Lomas, *CJEU Ruling on Meta Referral Could Close the Chapter on Surveillance Capitalism*, TECHCRUNCH, Jul. 4, 2023, https://techcrunch.com/2023/07/04/cjeu-meta-superprofiling-decision/ (last visited Jul 16, 2023). *See* Trevisan & Cuonzo - Caio Nunes, *CJEU Lands Groundbreaking Decision on Data Protection and Antitrust*, LEXOLOGY, Jul. 7, 2023, https://www.lexology.com/library/detail.aspx?g=e722bd9d-5135-4536-90aa-5b58c4a268d7 (last visited Jul 16, 2023). *See* CJEU decision in Facebook proceeding: Bundeskartellamt may take data protection rules into consideration, BUNDESKARTELLAMT (2023), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/04_07_2023_EuGH.html (last visited Jul 16, 2023). *See* Foo Yun Chee, *Meta Loses as Top EU Court Backs Antitrust Regulators over Privacy Breach Checks*, REUTERS, Jul. 5, 2023, https://www.reuters.com/technology/german-antitrust-watchdog-can-add-privacy-breaches-meta-probe-eu-court-says-2023-07-04/ (last visited Jul 16, 2023).

their considerations.[1018] Indeed, the erosion of consumer autonomy via manipulative OBA poses a systematic threat to consumer welfare, which is the primary aim of the EU competition law.[1019] Therefore, competition law has solid potential for mitigating the harms of consumer manipulation of OBA.[1020] Nevertheless, platforms and the digital technologies they rely on (e.g., AI and the markets they create) are characterized by intricacies that arguably create a need for more tailored forms of *ex-ante* regulation. Section 6.1.4 addresses the series of adopted and proposed legislation in the EU to complement and fill the gaps in consumer protection, personal data protection, and competition law. This legislation covers vast areas but converges in the intention to create the EU Digital Single Market and mitigate the adverse effects of digital technologies on human rights.

6.1.4. EU Digital Single Market[1021]

The EU addresses OBA's harms using various mechanisms as part of the "Digital Single Market Strategy" with so-called "dual objectives" to protect consumer interests and to promote integration, competitiveness, and growth of the EU single market for digital services.[1022] Essential is the package of the Digital Services Act (DSA) and Digital Markets Act (DMA) introduced in 2022. This section provides an overview of these mechanisms in relation to OBA and is further divided into three sub-sections: section 6.1.4.1 explains legal mechanisms that existed prior to the introduction of the DSA and the DMA; section 6.1.4.2 analyses the DSA and the DMA; and section 6.1.4.3 explains legislative initiatives regarding Artificial Intelligence Act (AIA).

6.1.4.1 Before the DSA and the DMA

The Audio Visual Media Services Directive (AVMSD) regulates audio-visual content, including advertising, presented by legacy media (i.e., radio, television)

[1018] *See* Graef, *supra* note 46. Davola and Malgieri, *supra* note 35. *See also* Nicholas Economides & Ioannis Lianos, *Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective*, 17 J. COMPET. L. ECON. 765 (2021).

[1019] *See* Graef, *supra* note 46 at 495–504.

[1020] *See Id.*

[1021] This chapter does not cover intellectual property, product safety, and non-discrimination laws. *See* section 1.4 and introduction to section 6.1.

[1022] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of the Regions A Digital Single Market Strategy for Europe COM (2015) 192, (2015). ("A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally.")

broadcasting and on-demand services (e.g., Spotify, Netflix).[1023] In 2018, the AVMSD was updated to cover video-sharing platforms, such as YouTube, Instagram, and TikTok, which, in practice, primarily fund their services via OBA.[1024] The AVSMD provides some restrictions for advertising content (e.g., for tobacco and alcohol products).[1025] Generally, rules regarding copyright, counterfeit goods, trademarks, and certain goods (e.g., alcohol, pharmaceuticals) and services (e.g., financial, gambling) create a plethora of restrictions for advertising, including OBA content.[1026] The AVMSD also provides rules for advertisement delivery that are particularly relevant for OBA. In particular, it requires platforms to ensure that advertisements are recognizable as such, prohibiting hidden advertising.[1027] It prohibits the use of subliminal techniques.[1028] The AVSMD also provides robust protections for minors: Article 6a of the AVMSD directly prohibits the collection and processing of the personal data of minors for commercial purposes, including for "behaviorally targeted advertising".[1029] Article 28(b)(3) AVMSD reiterates the prohibition of OBA directed towards minors, particularly for video-sharing platforms.[1030]

In 2019, the EU passed the Digital Content Directive (DCD) and Platforms to Business Regulation (P2BR), which acted as transitional legal mechanisms to address some of the challenges raised by the intermediation capabilities of platforms. The DCD provides that personal data could be a "counter-performance" for contracts instead of monetary payment, making the contracts for "free" digital content or services subject to consumer protection rules.[1031] In other words, the DCD ensures that consumers are protected through consumer protection rules within

[1023] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) 2010 O.J. (L 95) [hereinafter Audiovisual Media Services Directive], 1(a)(i)–(ii), (g). AVMSD distinguishes between "linear" and "non-linear" services. Linear services include traditional TV broadcasting that are provided at a "scheduled time, ad watched simultaneously by viewers". Non-linear or on-demand services provide audiovisual media to be watched at their own convenience. *See* EU audiovisual and media policies, EUROPA, https://ec.europa.eu/archives/information_society/avpolicy/reg/tvwf/provisions/scope/index_en.htm (last visited Jul 17, 2023).

[1024] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, 303 OJ L (2018).

[1025] *Id.* arts. 9(b), 11(4). *See also* Zard and Sears, *supra* note 1 at 40.

[1026] *See* Zard and Sears, *supra* note 1 at 40.

[1027] Audiovisual Media Services Directive, *supra* note 1025 art. 9(1)(a).

[1028] *Id.* art. 9(1)(b).

[1029] *Id.* art. 6a.

[1030] *Id.* art. 28(b)(3).

[1031] *See* Digital Content Directive, *supra* note 940.

the EU when they receive OBA-funded digital services and content without monetary payment. The P2BR aims to protect platform business customers and is a regulatory reaction to the European Commission finding Alphabet unfairly self-preferencing its services in the *Google Shopping* antitrust case 2017.[1032] The P2BR sets out the rules for platforms (e.g., Google Shopping) to inform its business users (e.g., wanting to sell on Google Shopping) about the ranking criteria, including whether ranking is sponsored, whether personalization takes place, and whether it is based on consumer behavior.[1033] The P2BR attempts to address power asymmetries between platforms and smaller businesses, including in the context of paid ranking (which can be a form of OBA), by increasing transparency and fairness.[1034]

6.1.4.2 The DSA and the DMA

In 2022, the EU adopted the Digital Services Act (DSA)[1035] and the Digital Markets Act (DMA),[1036] which provide the central pieces of legislation in the digital sector of the EU. These acts intend to respond to blind spots left by consumer protection, personal data protection, and competition law to safeguard against the harms of digital services and "create a safer and more open digital space" for EU consumers.[1037]

Depending on their impacts, the DSA introduces three layers of obligations for different kinds of digital service providers. In particular, the DSA sets baseline, first-layer rules for all platform service providers to establish a point of contact, report criminal offenses, and have user-friendly terms and conditions.[1038] The DSA singles out "online platforms" as a particular form of platform service that allows consumers to disseminate information to the public.[1039] Such a definition of "online platform" includes social networks, video-sharing services, and online marketplaces (excludes search engines and messaging apps) where these platform services can potentially be used to reach an unlimited number of consumers.[1040] In addition to

[1032] AT.39740 - Google Shopping, *supra* note 998.

[1033] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, 2019 O.J. (L 186) 57 [hereinafter P2B Regulation].

[1034] Commission Notice, Guidance on Ranking Transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, O.J. 2020 (C 424) 1. *See* Zard and Sears, *supra* note 1 at 46.

[1035] Digital Services Act, *supra* note 2.

[1036] Digital Markets Act, *supra* note 14.

[1037] *See The Digital Services Act package, Shaping Europe's digital future,* EUROPEAN COMMISSION (2023), https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last visited Apr 28, 2023).

[1038] The DSA refers to "intermediation service" providers (GLOSSARY). *See* Digital Services Act, *supra* note 2, recs. 7–15.

[1039] *Id.* rec. 13.

[1040] *Id.*

baseline, rules applied to all platform services, the DSA requires "online platforms" to engage in content moderation. These rules include, among other things, notice and action mechanisms, complaint handling systems, and out-of-court dispute resolution.[1041] Lastly, the DSA includes a third layer of obligations for "Very Large Online Platforms" (VLOPs) and Very Large Online Search Engines" (VLOSEs).[1042] On April 25, 2023, the European Commission designated seventeen VLOPs and two VLOSEs according to the rules of Article 33 DSA.[1043] These VLOPs and VLOSEs were selected because they serve at least 45 million EU consumers yearly (this number may change in the future to ensure it keeps reflecting 10% of the EU population)[1044]

The DMA includes a different classification of digital services. In particular, within platform services, it identifies "core platform services" that not only include "online platforms" in the meaning of the DSA, such as social networks, video-sharing platforms, and online marketplaces, but also search engines, cloud services, operating systems, web browsers.[1045] Particularly relevant for this thesis is that the DMA also covers advertising services, including advertising networks, advertising exchanges, and other advertising intermediaries, such as, inter alia, Demand Side Platforms (DSPs) or Supply Side Platforms (SSPs), given that a provider of such advertising services also provides another core platform service (e.g., search engine, online platform). [1046] Even then, the DMA does not apply to all core platform service providers but only to those providers that are designated as "gatekeepers" according to Article 3 DMA.

One of the criteria for such designation is similar to designating VLOPs and VLOSEs, regarding the number of active users being 45 million a year. However, the designation process in the DMA also includes the evaluation of further qualitative and quantitative criteria. For example, one quantitative criterion looks at whether the yearly turnover of the core platform service provider in the EU amounts

[1041] The DSA refers to "intermediation service" providers (see *GLOSSARY*). *See Id.* recs. 7–15.

[1042] The DSA builds on the landmark e-Commerce Directive of 2000 and primarily includes intermediation liability rules for online businesses. Nevertheless, the DSA gives particular importance to digital platforms (including search engines) due to their reach, and, therefore, imposes special obligations to them. *See* Digital Services Act, *supra* note 38, recs. 75-76. The DSA adopts the threshold of 45 million active monthly users. Further, DSA distinguishes Very Large Online Platforms (VLOP)s and Very Large Online Search Engines (VLOSEs).

[1043] Digital Services Act, *supra* note 38, art. 33. 17 VLOPs: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Maps, Google Play, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando; 2 VLOSEs: Google Search, Microsoft Bing. *See* DSA: Very Large Online Platforms and Search Engines, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 (last visited Apr 28, 2023).

[1044] Digital Services Act, *supra* note 2, art. 33.

[1045] Digital Markets Act, *supra* note 14, art.2(2).

[1046] *Id.*

to at least €7,5 billion.[1047] For designating gatekeepers, it is essential that such core platform providers hold a particularly "durable" and "entrenched" position. [1048] Designated gatekeepers and VLOPs/VLOSEs are overlapping concepts. In case core platform services that gatekeepers provide are "online platforms" and "online search engines", they are also VLOPs/VLOSEs. However, VLOPs/VLOSEs are not always gatekeepers (e.g., Snapchat) because they do not meet further Article 3 DMA criteria.[1049] The DMA addresses structural harms on the market stemming primarily from the "data power" of designated gatekeepers and promotes contestability and fairness in the EU single market.[1050]

The DSA and the DMA include several provisions that set boundaries for consumer manipulation via OBA. The EU legislator considered the complete ban on OBA when advertising relied on processing consumers' data in the DSA.[1051] However, the final text of the DSA prohibits "online platforms" from engaging in OBA when: (i) "when they are aware with reasonable certainty that the recipient of the service is a minor"[1052] or (ii) when they process special categories of data" (as defined under the GDPR).[1053] The DSA justifies these prohibitions of OBA targeted to minors and using sensitive data as having a potential for exploitation of vulnerabilities and manipulation, creating higher societal risks.[1054]

Article 26 (1) DSA provides increased transparency requirements on remaining forms of OBA, including an obligation to disclose (a) the advertisement as such, (b) on whose behalf the ad is presented (i.e., advertiser), (c) who pays for an ad if not the advertiser (e.g., an advertising network) and (d) the main parameters used for

[1047] The designation of "gatekeepers" is more nuanced. Gatekeepers have to satisfy three conditions: firstly, they (a) have to have a "significant impact on the internal market". Such impact can be confirmed if their turnover for three years before evaluation constituted €7,5 billion or if market capitalization reached €75 billion. Secondly, (b) they have to provide one of the core services – this can be similar to VLOPs (45 million users) or 10 000 yearly business users. Lastly, (c) it has to have a "durable" position in the market, meeting the thresholds for three consecutive years. *See* Digital Markets Act, *supra* note 14, art. 3.

[1048] *See* Johann Laux, Sandra Wachter & Brent Mittelstadt, *Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA*, 43 COMPUT. L. SECUR. REV. 105613 (2021).

[1049] On July 4, 2023 the European Commission published 7 potential gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, Samsung. *See Here are the first 7 potential "Gatekeepers" under the DMA*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_3674 (last visited Jul 22, 2023).

[1050] *See* Digital Markets Act, *supra* note 14, rec. 36. at rec. 69.

[1051] Digital: EU must set the standards for regulating online platforms, say MEPs, EUROPEAN PARLIAMENT (2020), https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps (last visited Apr 28, 2023).

[1052] *See* Digital Services Act, *supra* note 2, art. 28(2).

[1053] *Id.* art. 26.

[1054] *Id.* rec. 69.

targeting, including, if applicable, information on how to change these parameters.[1055] Similarly, the DSA imposes transparency requirements if the content is personalized.[1056] It is likely, but not certain, that Article 26(1) DSA transparency requirements and prohibitions also apply to VLOSEs, which are not necessarily "online platforms" under the definition of DSA. In addition, the DSA requires VLOPs/VLOSEs to provide a public repository of the advertisements shown on their websites for further transparency.[1057] Digital Service Coordinators (DSCs), authorities in the Member States charged with the enforcement of the DSA, and the European Commission can scrutinize the data and algorithms that VLOPs/VLOSEs employ.[1058] The DSA requires the European Commission to encourage the development of voluntary codes of conduct for actors in the online advertising ecosystem, including advertising intermediaries, by February 2025 in order to create a "competitive, transparent, and fair environment in online advertising".[1059]

The DMA sets further boundaries on OBA by restricting how gatekeepers use personal data and prohibiting them from combining data from different platforms and third parties without consumers' consent.[1060] This DMA prohibition echoes the *Meta v. Bundeskartellamt* logic that prohibited Meta from combining data between WhatsApp, Instagram, and Facebook and requires gatekeepers to integrate such data only when the consumer consented (section 6.1.3).[1061] The DMA also clarifies that gatekeepers can ensure such consent is freely given by "offering a less personalized but equivalent alternative."[1062] The DMA mentions consumer choice 23 times, and safeguarding consumers against exploitation through manipulative and coercive practices is one of its main objectives. Offering a less personalized but equivalent alternative is supposed to ensure that if consumers accept an OBA-funded alternative, that is actually what they want. From the framework of influence developed in this thesis, this means that gatekeepers have to offer at least one alternative that is also without monetary payment.

The DMA includes a variety of rules for gatekeepers as advertising intermediaries to ensure contestability and fairness in the OBA ecosystem.[1063] In the context of the OBA, the central logic of the DMA is to limit the gatekeepers' data

[1055] *Id.* art. 26.
[1056] *Id.* art. 27.
[1057] *Id.* art. 39.
[1058] *Id.* art. 40.
[1059] *Id.* art. 46.
[1060] Digital Markets Act, *supra* note 14, art. 5(2).
[1061] BKartA, Case VI-Kart 1/19 (V), Facebook (Ger.), *supra* note 1015.
[1062] Digital Markets Act, *supra* note 14, rec. 36.
[1063] *Id.* at 5.

power and make the ecosystem more contestable, affecting the potential to manipulate consumers.[1064]

The DMA provides an *ex-ante* legislative instrument that can significantly affect the power in the digital sector, including in the advertising market. However, the DMA also presents a risk that increasing contestability in the markets based on the infrastructure in which manipulation is incentivized can exacerbate consumer manipulation by expanding the capabilities of the platform service providers of such manipulation to other actors of the OBA infrastructure, including smaller platform providers and publishers.

6.1.4.3 Artificial Intelligence Act (AIA)

In 2022, the European Commission proposed the Artificial Intelligence Act (EC.AIA), which also may set boundaries for consumer manipulation via OBA.[1065] OBA relies on AI systems in various ways, including predicting the quality score of an advertisement, inferring consumers' interests, and deciding which consumer to target (section 2.1). The EC.AIA introduces a risk-based approach to regulating AI systems. It prohibits AI systems with unacceptable risk, sets mandatory compliance requirements for AI systems with high risk, and sets transparency rules for low or minimal-risk AI systems. The EC.AIA does not single out AI systems used in OBA as either high risk or as one of the unacceptable practices.

This may suggest that AI used in OBA is a low or minimal-risk system. If this were the case, Article 52 EC.AIA requires providers of such AI systems to inform natural persons it interacts with about it being an AI system.[1066] Article 56 EC.AIA establishes the European Artificial Intelligence Board (EAIB) as an authority providing guidance regarding EC.AIA in the EU.[1067] Article 69 EC.AIA requests the EAIB and the European Commission to "encourage" and "facilitate" the creation of codes of conduct that low-risk AI system providers would voluntarily join to meet the requirements of the high-risk AI systems.[1068] Articles 6-51 EC.AIA contain specific provisions for the providers of AI systems that pose an increased risk to health, safety, or fundamental rights. Annex III provides the list of high-risk AI systems.[1069]

Most relevant for this thesis is Chapter 1 of the EC.AIA, which lists AI systems with unacceptable risks. In particular, Article 5 (1)(a) EC.AIA prohibits using AI

[1064] The Commission's proposal for Data Act has a similar imperative. Barbbara da Rosa Lazarotto & Gianclaudio Malgieri, *The Data Act: A (Slippery) Third Way Beyond Personal/Non-Personal Data Dualism?*, EUROPEAN LAW BLOG (2023), https://europeanlawblog.eu/2023/05/04/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/ (last visited May 10, 2023).

[1065] AI Act Proposal, *supra* note 52.

[1066] *Id.* rec. 52.

[1067] *Id.* rec. 69.

[1068] *Id.* rec. 56.

[1069] *Id.* annex III.

that relies on "subliminal techniques",[1070] and Article 5(1)(b) exploits vulnerabilities of specific groups and can "materially distort a person's behavior".[1071] These prohibitions can act as explicit prohibitions of consumer manipulation, including in the context of OBA, and are discussed further in section 6.2.5. One limitation of these prohibitions is that they only apply when manipulation leads to physical and psychological harm.[1072] Another limitation is that while AI can exploit various internal and external vulnerabilities in all humans, the text focuses on vulnerabilities associated with groups (e.g., minors), and such a choice can leave the core of the manipulation harms unaddressed by the provisions.

In June 2022, the European Parliament published its amendments for the proposed AIA (EP.AIA), suggesting several amendments to the EC.AIA that substantively expands the prohibitions.[1073] In particular, Article 5(1)(b) EP.AIA introduces amendments that remove the benchmark of "physical and psychological" harm and instead prohibit practices that can cause "significant harm." They replace the concept of label or group vulnerability in the Article 5 EC.AIA with a layered vulnerability that includes personality traits and economic situation, among other vulnerabilities that AI systems can exploit. Article 5(1)(a) EP.AIA expands purposeful manipulation to use AI systems in a way that has "the effect of" manipulation and seems to include societal harm. Lastly, the EP.AIA added recommender systems of VLOPs as defined by the DSA to be high-risk AI systems.

To sum up section 6.1, consumer manipulation via OBA is regulated through various legal instruments in consumer protection, personal data, privacy protection, competition law, and digital single market strategy. While looking at these fields of law separately provides only a limited view of the legal boundaries of consumer manipulation via OBA, a holistic view reveals a clearer picture of how these boundaries safeguard against the harms identified in Chapter 5 of this thesis. Therefore, sections 6.2-6.6. analyze the synergies between the EU legal framework elaborated in section 6.1 and the boundaries they are able to set for consumer manipulation via OBA.

[1070] *Id.* art. 5(1)(a). (prohibiting "the placing on the market [and] putting into putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm").

[1071] *Id.* art. 5(1)(b) (prohibiting "the placing on the market" and "putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm").

[1072] *Id.* art. 5(1)(a)-(b).

[1073] AI Act Mandates, *supra* note 367.

6.2. Prohibited OBA Practices

Academia,[1074] civil society,[1075] media,[1076] and politicians[1077] have called for an outright ban on OBA because it is fundamentally irreconcilable with democratic values and human rights. The *Tracking-Free Ads Coalition* has advanced this agenda in the European Parliament, which, in the discussions around the DSA, called for first prohibiting "micro-targeting" and starting a phase-out of OBA entirely, leading to its ultimate prohibition.[1078] The European Data Protection Supervisor (EDPS) also backed the European Parliament, inviting the European Commission to prohibit OBA via "pervasive tracking ultimately."[1079]

In response to the growing potential of their monetization scheme being explicitly outlawed, the OBA industry led by Alphabet and Meta has engaged in intensive lobbying and used *targeted advertising* to influence European politicians.[1080] The industry's strategy, similar to one that arguably stalled ePrivacy Regulation,[1081] emphasizes potentially disastrous consequences to Small and Medium Size Enterprises (SMEs) that OBA allegedly allows to fund by helping

[1074] *See e.g.,* Robert Hackett, *Harvard Economist Calls to Outlaw Online Advertising Markets—Just Like "Organs, Babies, or Slaves,"* FORTUNE, Nov. 18, 2019, https://fortune.com/2019/11/18/google-facebook-online-advertising-ban-surveillance-capitalism/ (last visited May 6, 2023).

[1075] *See e.g.,* FORBRUKERRADET, TIME TO BAN SURVEILLANCE ADVERTISING (2021). *See* also Ban Surveillance Advertising, BAN SURVEILLANCE ADVERTISING, https://www.bansurveillanceadvertising.com/ (last visited May 6, 2023). *See also* Surveillance giants: How the business model of Google and Facebook threatens human rights, AMNESTY INTERNATIONAL (Nov. 21, 2019), https://www.amnesty.org/en/documents/pol30/1404/2019/en/ (last visited May 6, 2023). *See also* EU: Put Fundamental Rights at Top of Digital Regulation, HUMAN RIGHTS WATCH (Jan. 7, 2022), https://www.hrw.org/news/2022/01/07/eu-put-fundamental-rights-top-digital-regulation (last visited May 6, 2023).

[1076] *See e.g.,* Gilad Edelman, *Why Don't We Just Ban Targeted Advertising?*, WIRED, Mar. 2020, https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/ (last visited May 6, 2023).

[1077] *See e.g.,* Facebook does not make the laws! S&Ds Launch Pan-European Campaign To Stop Online Data Abuse, SOCIALISTS & DEMOCRATS (Feb. 22, 2021), https://www.socialistsanddemocrats.eu/newsroom/facebook-does-not-make-laws-sds-launch-pan-european-campaign-stop-online-data-abuse (last visited May 6, 2023).

[1078] *See* Tracking-Free Ads Coalition, https://trackingfreeads.eu/ (last visited May 5, 2023). *See* European Parliament Resolution of 18 June 2020 on Competition Policy, 2021 O.J. (C 362) 22, 35 ¶ 105.

[1079] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 1/2021 On the Proposal For A Digital Services Act 3*, 1 (2017).

[1080] Corporate Europe Observatory, *How the European Parliament's Proposals on Surveillance Advertising Changed Over Time*, 2022, https://corporateeurope.org/en/2022/01/how-corporate-lobbying-undermined-eus-push-ban-surveillance-ads (last visited May 5, 2023).

[1081] *See* Corporate Europe Observatory, *Big Data Is Watching You* (2017), https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you (last visited May 6, 2023).

them reach their audiences.[1082] Ultimately, the European Commission avoided proposing the outright prohibition of OBA in the DSA.[1083]

Nevertheless, the EU legal framework includes a variety of explicit prohibitions that set legal boundaries for consumer manipulation via OBA. This section analyzes these prohibitions, starting with the most specific (to manipulation via OBA) to the most general (unfair commercial practices): section 6.2.1 evaluates the prohibition of relying on special categories of data for OBA; section 6.2.2 elaborates on the prohibition of OBA targeted to minors; section 6.2.3 analyzes the prohibition of automated decision-making in the GDPR; and section 6.2.4 evaluates the general prohibition of consumer exploitation in the UCPD. Lastly, section 6.2.5 elaborates on proposed prohibitions of using manipulative AI for OBA.

6.2.1. The Prohibition of OBA Using Special Categories of Data

The DSA sets explicit boundaries for consumer manipulation via OBA.[1084] It recognizes that "[i]n certain cases, manipulative techniques [in OBA] can negatively impact entire groups and amplify societal harms, for example, by contributing to disinformation campaigns or by discriminating against certain groups."[1085] With this in mind, and by considering the high societal risk posed by "online platforms" (as defined by the DSA), Article 26(3) DSA prohibits providers of these platforms from presenting advertisements using special categories of personal data (as defined by the GDPR).[1086] Such data includes, inter alia, consumers' political opinions, sexual preferences, or health.[1087] In its narrowest interpretation, Article 26(3) DSA suggests that these platforms cannot target consumers based on sensitive profile categories (e.g., sexual orientation). Indeed, since 2021, Alphabet and Meta have already stopped providing such explicit targeting options on their platforms.[1088]

The grammatical interpretation of Article 26(3) DSA suggests a bit broader scope of the prohibition.[1089] As Recital 69 DSA explains, Article 26(3) prohibition *includes,* but is not limited to, prohibiting OBA that is personalized "using profiling categories based on those special categories".[1090] Instead, Article 26(3) DSA prohibits "online platforms" from presenting any advertisements "based on profiling

[1082] *See* Corporate Europe Observatory, *supra* note 1082.

[1083] *See* CEOs make final push to ban targeted ads, POLITICO (Jan. 13, 2022), https://www.politico.eu/article/activist-ceo-mep-crack-down-targeted-ads-vote-digital-services-act-2/ (last visited May 8, 2023).

[1084] *See* Digital Services Act, *supra* note 2 rec. 69.

[1085] *See* Digital Services Act, *supra* note 2 rec. 69.

[1086] *See Id.* art. 26(3), rec. 81.

[1087] *See* General Data Protection Regulation, *supra* note 44 art. 9.

[1088] *See* Removing Certain Ad Targeting Options and Expanding Our Ad Controls, *supra* note 775; Personalized Advertising, *supra* note 120.

[1089] *See* Digital Services Act, *supra* note 2 art. 26(3) rec. 81.

[1090] *See Id.,* rec. 69.

[…] *using* special categories of personal data" (emphasis added), suggesting that such data cannot be processed to present personalized advertisements at all.[1091] Such a reading shifts focus on identifying what it means to process special categories of data (under Article 9 GDPR) in the context of OBA. This can be argued to include not only placing a consumer into a special category (e.g., sexual orientation) but also inferring affinity interests (e.g., interest in LGBTQ+ rights).[1092] Yet, an even broader interpretation can be that Article 9 GDPR applies when data (e.g., pornographic browsing history) reveals sensitive attributes.[1093] The broadest interpretation suggests that any data (e.g., mouse cursor movement) can be a special category of data if there is a way to infer information about protected attributes.[1094]

The case law of the CJEU regarding Article 9 GDPR provides limited guidance: the test in assessing whether data belongs to a special category is whether data *reliably* (not certainly) reveals sensitive information.[1095] In Case T-190/10 *Egan & Hackket,* the CJEU found that knowledge that a person works as an assistant to a member of the European Parliament does not reliably reveal his political leanings.[1096] In contrast, in Case C-184/20 *OT,* the CJEU recognized that knowing the spouse's full name reliably revealed the person's sexual orientation.[1097] In *OT judgment,* the CJEU further explained that data belongs to special categories if "by means of an intellectual operation involving comparison or deduction," this data reveals sensitive information.[1098] These decisions reveal blurry lines to understand when non-sensitive data has to be reclassified as special categories of data. This is particularly the case for OBA, in which personalization based on any behavioral data (e.g., cursor movements) may act as a proxy and implicitly reveal some sensitive attribute (e.g., Alzheimer's disease).[1099]

The broadest interpretation may lead to an argument that all OBA involves the processing of special categories of data and is, thus, prohibited. However, the fact that the European Commission rejected the option to directly and entirely prohibit OBA in the DSA reveals that the goal of the regulator was to place a different,

[1091] *See* Digital Services Act, *supra* note 2, art. 26(3), rec. 81.

[1092] This gray area of Article 9 GDPR is discussed in detail by Wachter. *See* Wachter, *supra* note 80 at 383.

[1093] *Id.* at 382.

[1094] *See* Tal Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. (2017).

[1095] *See* Wachter and Mittelstadt, *supra* note 579 at 75.

[1096] Case T-190/10, *Egan & Hackett v. Parliament*, 28 March 2012, ECLI:EU:T:2012:165.

[1097] Case C-184/20, *Vyriausioji tarnybinės etikos komisija*, August 1, 2022, ECLI:EU:C:2022:601. (2022).

[1098] *Id.*

[1099] *See* Wachter and Mittelstadt, *supra* note 579 at 75. *See also* Veale and Zuiderveen Borgesius, *supra* note 31 at 242. *See also* CPDPConferences, *supra* note 945.

relatively milder boundary.[1100] Precise boundaries will remain blurred until further CJEU interpretations of Article 9 GDPR or Article 26(3) DSA. Two potential interpretations are that (1)"online platforms" are allowed to process consumer behavioral data for OBA (e.g., pornographic browsing history) as long as they do not *intend* to use the data to identify attributes that are sensitive explicitly (e.g., sexual orientation) or by inference (e.g., interest in LGBTQ+ community); or that (2) "online platforms" are prohibited from processing consumer behavior data for OBA unless they demonstrate that the data *can* not reveal special categories.

The *first* interpretation stands on the premise that behavioral data do not belong to special categories because the intention of online platforms to infer sensitive attributes is absent.[1101] There is no legal consensus that *intentionality* is a necessary condition for regarding the data to belong to special categories.[1102] The intentionality argument suggests that a pizzeria delivering pizza to a consumer in a rehab facility does not process special categories of data unless the pizzeria intends to infer information about the health status of its consumers.[1103] This thesis argues that in the context of OBA, it is irrelevant whether or not intentionality criteria are a pre-condition for reclassifying personal data as belonging to special categories because OBA would satisfy such criteria. This argument can be made by teleological analysis of Article 26(3) DSA and Article 9 GDPR provisions in light of consumer manipulation via the OBA framework developed in this thesis.

It is evident from Recital 69 DSA that Article 26(3) DSA aims to mitigate consumer manipulation via OBA.[1104] This effect of OBA can arise when platform providers deliberately target to exploit consumer vulnerabilities (that at times reflect sensitive attributes), but also if they disregard that their algorithms are likely to exploit consumer decision-making vulnerability.[1105] Through OBA, platform providers intend to maximize profit by displaying the ads the consumer is most likely to act on (section 2.5). Therefore, even though platform providers may not deliberately target sensitive attributes, they can be said to *intend* to do so in case they disregard that the algorithmic systems they deploy can process special categories of data. For example, the feature of "similar audiences" ("lookalike audiences") could implicitly target consumers with Alzheimer's disease based on the

[1100] *See* Tracking-Free Ads Coalition, *supra* note 1080. *See* European Parliament Resolution of 18 June 2020 on Competition Policy, 2021 O.J. (C 362) 22, 35 ¶ 105., *supra* note 1080. *See also* Corporate Europe Observatory, *supra* note 1082.

[1101] Wachter and Mittelstadt, *supra* note 579 at 75.

[1102] *Id.*

[1103] *Id.*

[1104] Recital 69 DSA reveals that the aim of Article 26(3) DSA is to set boundaries for the capability of "online platforms" to manipulate consumers via OBA and safeguard against harms such as disinformation or discrimination. *See* Digital Services Act, *supra* note 2, rec. 69.

[1105] *See generally* Klenk, *supra* note 305.

inference that consumers with "similar" mouse movements are more likely to click on the advertisement.[1106]

With this in mind, a *second* interpretation that Article 26(3) DSA prohibits "online platforms" from processing consumer behavior data for OBA unless they demonstrate that the data *can* not reveal special categories seems more aligned with the regulator's goals.[1107] This would suggest that these platform providers must actively identify possibilities through which data they process can belong to special categories and make sure they do not process such data. However, ensuring that consumer data processed for OBA can not reveal special categories of data may be technically impossible.[1108] Therefore, such an interpretation may require "online platforms" to stop practices such as "similar audiences", in which they cannot guarantee that data does not turn into special categories of data.

As long as the boundaries of Article 26(3) DSA remain blurred, the industry is likely to adopt a milder boundary and stop their OBA practices from being targeted at the categories that are sensitive explicitly (e.g., sexual orientation) or by inference (e.g., interest in LGBTQ+ community). However, Article 39 DSA provision regarding additional advertising transparency requirements of VLOPs and VLOSEs (such as some of the platforms of Alphabet and Meta) can give way to a stricter interpretation of Article 26(3) DSA . In particular, Article 39 DSA requires VLOPs and VLOSEs to provide public advertising repositories where enforcers and the general public can analyze individual advertising campaigns in their OBA practices, including to what extent they process special categories of data (section 6.1.4.2).[1109]

The primary challenge or shortcoming of Article 26(3) DSA is that the provision focuses on "special categories of data" and not the problem itself.[1110] The problem at hand is consumer manipulation (and exploitation) harms of OBA. Addressing the categories of data instead of directly focusing on the manipulation can be an ineffective way to resolve the problem.[1111] Therefore, not only does Article 26(3) DSA draw a blurry boundary of what kind of data "online platforms" can process for OBA, but even if it is clearly delineated, it may not adequately capture all ways consumer vulnerabilities can be exploited. For example, if

---

[1106] *See e.g.,* Ryen W. White, P. Murali Doraiswamy & Eric Horvitz, *Detecting Neurodegenerative Disorders from Web Search Signals*, 1 NPJ DIGIT. MED. 8 (2018).

[1107] *See Meta v Bundeskartellamt*, *supra* note 1017, 88. ("[W]here a set of data containing both sensitive data and non-sensitive data is subject to such operations and is, in particular, collected en bloc without it being possible to separate the data items from each other at the time of collection, the processing of that set of data must be regarded as being prohibited, within the meaning of Article 9(1) of the GDPR, if it contains at least one sensitive data item.")

[1108] Solove, *supra* note 631 at 4.

[1109] *See* Digital Services Act, *supra* note 2, rec. 69.

[1110] Solove criticizes "special categories of data" paradigm. *See generally* Solove, *supra* note 631.

[1111] *Id.*

consumers are exploited by relying on the correlation that Apple users pay more than Windows/Android users, this will not constitute processing of special categories of data and, therefore, outside of Article 26(3) DSA scope. In contrast to such a limiting focus on special categories of data, the EC.AIA proposed directly addressing manipulation via AI systems (section 6.2.5). In this respect, the UCPD prohibition of unfair practices is the most inclusive formulation against consumer exploitation (section 6.2.4).

Another challenge with the Article 26(3) DSA is that the prohibition only applies to "online platforms".[1112] This means that other digital service providers are not explicitly prohibited from using special categories of data for their OBA practices. This may seem to be a loophole.[1113] It is likely that the regulator left this gap to relieve more minor actors from the regulatory burden. Such actors that are not "online platforms" include advertising intermediaries and other publishers (e.g., online newspapers). This gap is understandable if Article 26(3) DSA is read together with Article 46 DSA and Article 5 UCPD provisions. In particular, Article 46 DSA refers to "online advertising codes of conduct" that the European Commission is called to "encourage" the industry to commit to voluntarily.[1114] By establishing in codes of conduct (under Article 46 DSA) that OBA with special categories of data is prohibited, digital service providers that are not "online platforms" can be held liable under Article 5(2) UCPD to breach their "professional diligence" in case they process such data.[1115] Article 46 DSA codes of conduct will apply from 18 August 2025.[1116]

In sum, Article 26(3) DSA sets a blurry boundary between legally acceptable and unacceptable OBA practices by prohibiting "online platforms" from using special categories of data for OBA. Recital 69 DSA reveals that the regulator aimed to mitigate against some of the consumer manipulation harms of OBA (e.g., disinformation). Indeed, Article 26(3) DSA can potentially be interpreted to mitigate such harms, but focusing on "special categories of data" is not the most appropriate way to prohibit consumer manipulation via OBA. Practical application of Article 26(3) DSA will require operationalizing other DSA provisions, such as Article 39 DSA, requiring VLOPs/VLOSEs to keep repositories, and Article 46 DSA, requiring other digital service providers to adopt advertising codes of conduct. Even then, the ultimate safety net for consumer manipulation via OBA is the UCPD.

[1112] In essence, DSA's definition of "online platforms" does not include "online search engines." Section 3 where advertising requirements are listed applies only to online platforms. Section 3 is likely also to apply for VLOSEs, therefore, covering Google Search and Microsoft Bing.

[1113] *See generally* Hacker, *supra* note 54.

[1114] Digital Services Act, *supra* note 2, art. 46.

[1115] Unfair Commercial Practices Directive, *supra* note 42, art. 5(2).

[1116] Digital Services Act, *supra* note 2, art. 46.

6.2.2. The Prohibition of OBA for Minors

The EU legal boundaries are more precise regarding targeting children – OBA cannot be targeted to minors: Article 8 of the GDPR requires all digital service providers to ensure minors have enhanced protections when processing their personal data.[1117] Recital 38 GDPR explicitly clarifies that such specific protections apply in the context of OBA.[1118] In 2018, the A29WP argued that OBA is not a suitable practice for children as they are particularly vulnerable to influences in an online environment.[1119] Also, in 2018, the updated text of the AVMSD included the explicit prohibition of video-sharing online platforms showing behaviorally targeted advertisements to minors.[1120] Lastly, Article 28(2) DSA introduced another explicit prohibition for "online platforms" to show OBA to minors "on their interface."[1121] Article 28(2) DSA applies not only to video-sharing online platforms such as YouTube, Instagram, and TikTok but also has further scope and includes all "online platforms" that allow public dissemination of digital content, including social networks (e.g., Facebook, X) or online marketplaces (e.g., Amazon).[1122]

Article 28(2) of the DSA prohibition suggests online platforms cannot show OBA to minors *on their interfaces*.[1123] The wording differs slightly from the Article 26(3) DSA prohibition for relying on sensitive data for OBA that does not mention the interface of online platforms but generally to the "recipients of service".[1124] This may suggest that the DSA relieves "online platforms" from the responsibility to parse between minors and adults when they provide advertisements to other publishers (e.g., online newspapers) via their advertising networks (e.g., Meta

[1117] General Data Protection Regulation, *supra* note 44, art. 8.

[1118] *Id.* rec. 38. ("Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regards to children when using services offered directly to a child.")

[1119] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated Individual Decesion-Making and Profiling for The Purposes of Regulation 2016/679*, 29 (2018). ("[c]hildren can be particularly susceptible in the online environment and more easily influenced by behavioral advertising", suggesting that businesses should "refrain from profiling them for marketing purposes")

[1120] Audiovisual Media Services Directive, *supra* note 1026 art. 6a(2). ("Personal data of minors collected or otherwise generated by media service providers[…] shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.")

[1121] European Parliament version of the DSA included firmer prohibition: "Targeting or amplification techniques that process, reveal or infer personal data of minors or personal data […] for the purpose of displaying advertisements are prohibited." *See* Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html (last visited Oct 16, 2023).

[1122] Digital Services Act, *supra* note 2, art. 28(2).

[1123] *Id.*, art. 28(2).

[1124] *Id.*, art. 26(3).

Audience Network). This does not mean minors can be targeted with OBA when accessing non-"online platform" publishers. Prior to the adoption of the DSA, there was a consensus among data protection authorities (DPAs) that personal data could not be processed for OBA targeted to minors by any of the digital service providers.[1125] While Article 28(2) DSA prohibition is limited to providers of "online platforms", Article 8 GDPR likely prohibits all digital service providers from processing personal data related to minors for OBA.[1126]

Therefore, the challenge is implementing and enforcing Article 28(2) DSA prohibition and Article 8 GDPR protections. The regulator is not explicit about how digital service providers must ensure differentiation between adults and minors who receive their service.[1127] In 2021, as a response to a minor committing suicide when engaging in behavior promoted by TikTok, the Italian (IT) DPA ordered ByteDance to block access to all Italian users "whose age could not be determined with full certainty to ensure compliance with age requirements."[1128] Adopting such a "full certainty" principle would mean that OBA is prohibited entirely unless digital service providers thoroughly verify the age of their consumers.

In contrast, Article 28(2) DSA clarifies that "online platforms" cannot engage in OBA when they are "aware with reasonable certainty" that the consumer is a minor.[1129] Further, Article 28(3) DSA clarifies that the prohibition of Article 28(2) DSA should not lead online platform providers to obtain more information to identify the consumer as a minor.[1130] As providers of "online platforms" are responsible for ensuring their OBA practices do not target minors, nor are they allowed to request additional data from their consumers to identify if they are minors, they must rely on privacy-friendly age verification tools.[1131] Providers of VLOPs, such as Instagram and TikTok, are likely to use algorithmic tools to predict whether a consumer is minor.[1132] It depends mainly on the enforcers and the extent to which they require digital service providers to comply with this requirement.[1133]

[1125] *See e.g.,* DATA PROTECTION COMMISSION, *Fundamentals for a Child-Oriented Approach to Data Processing*, (2021).

[1126] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 02/2013 on Apps on Smart Devices*, (2013).

[1127] Mihnea Dumitrascu, *DSA - Targeted Advertising Aimed at Minors: A Future Ban?*, BIRD & BIRD (Mar. 28, 2023), https://www.twobirds.com/en/insights/2023/global/dsa-publicite-ciblee-destinee-aux-mineurs-une-interdiction-a-venir (last visited May 8, 2023).

[1128] European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36.

[1129] Digital Services Act, *supra* note 2, art 28.

[1130] *See* Dumitrascu, *supra* note 1129.

[1131] Digital Services Act, *supra* note 2, art. 28(3).

[1132] *See* Introducing New Ways to Verify Age on Instagram, META (Jun. 23, 2022), https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/ (last visited Oct 16, 2023).

[1133] *See* Dumitrascu, *supra* note 1129.

The extent to which digital service providers must differentiate between minors and adults may differ. An online newspaper may state in its terms and conditions that its services are directed to adults and, indeed, the content of a publisher's website may relate to political news. In the A29WP interpretation of Article 8 GDPR, such digital services can be free from verifying consumer age.[1134] The same will not apply to publishers that provide video games or game apps likely to be accessed by minors. In particular, in gaming environments, OBA can lead to exploiting children's vulnerabilities.[1135] With this in mind, to comply with Article 8 GDPR, publishers providing such environments must refrain from OBA unless they verify that the consumer is an adult. With the limited availability of privacy-preserving verification tools, how strictly SAs will enforce Article 8 GDPR requirements, as well as Article 28(2) DSA and Article 6a (2) AVMSD prohibitions, remains to be seen.

6.2.3. The Prohibition of Profiling with Significant Effects

Article 6(1) GDPR lists legal grounds (e.g., consent) that must be met for any processing of personal data to be considered legitimate.[1136] In case OBA is targeted to adults and passes the test of Article 6(1) GDPR, which can in itself be tricky (section 6.3), the GDPR allows OBA unless it constitutes "automated decision-making, including profiling that has legal effects or otherwise significant effects" on the consumers.[1137] This prohibition in Article 22 GDPR reflects the data protection rules prior to the GPDR that were designed to restrict the use of computer systems for making decisions that could discriminate, for example, in the employment context.[1138] The recitals of the GDPR explicitly mention "automatic refusal of an online credit application" and "e-recruiting practices without human intervention" as examples of practices with *similar* significant effects.[1139] Still, the Article 22 provision is particularly ambiguous, has limited case law, and is widely debated in academia.[1140]

It is unclear the extent to which Article 22 GDPR applies to OBA for two reasons: firstly, it is unclear if algorithmic mediation of whether or not a consumer

[1134] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 1121 at 29. ("[c]hildren can be particularly susceptible in the online environment and more easily influenced by behavioral advertising", suggesting that businesses should "refrain from profiling them for marketing purposes")

[1135] van der Hof et al., *supra* note 876.

[1136] General Data Protection Regulation, *supra* note 44 art 22.

[1137] *Id.,* art 22.

[1138] *See* CHEN, *supra* note 947 at 122–123.

[1139] General Data Protection Regulation, *supra* note 44, rec. 71.

[1140] Andreas Hauselmann, *The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber*, EUROPEAN LAW BLOG (Feb. 20, 2023), https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/ (last visited May 9, 2023).

sees an advertisement can be considered a "decision" within the meaning of Article 22 GDPR, and secondly, even if it does, whether such a decision produces legal or similarly significant effects.[1141] In 2021, the Amsterdam District Court ruled in the so-called "Uber ADM Case" that algorithmic matching of the drivers and consumers did not constitute automated decision-making because the interests of drivers and consumers were not "significantly" affected.[1142] Also, in 2021, the so-called "Schufa Case" was referred to the CJEU to decide whether using a particular credit scoring system constitutes automated decision-making under Article 22 GDPR.[1143] The final judgment in the Schufa case is expected in late 2023.[1144] While this can clarify the scope of Article 22 GDPR, its application to OBA will likely remain provisional.

The A29WP argues that OBA, in essence, constitutes automated decision-making but that evaluating whether effects are significant in the context of OBA depends on *inter alia* whether cross-site and third-party tracking takes place and whether the vulnerabilities of consumers are known to the businesses.[1145] The A29WP also suggests that significance can be established if decisions affect financial circumstances, access to health services, employment opportunities, and education.[1146] Therefore, it is likely that that Article 22 GDPR is interpreted to apply at least when OBA is used to advertise financial products, health services, employment, housing opportunities, and price discrimination.[1147]

This thesis argues that Article 22 GDPR can be interpreted to cover OBA in cases in which there is a higher likelihood of consumer manipulation, which can be suggested to be a *significant* enough *effect* to be covered by Article 22 GDPR. Generally, the lack of relevant case law makes Article 22 GDPR a relatively weak vehicle for setting boundaries for consumer manipulation via OBA. However, Article 39 (2) DSA, which ensures additional transparency measures for VLOPs/VLOSEs, may help operationalize Article 22 GDPR. In particular, Article 39 (2) (e) DSA requires VLOPs/VLOSEs to make publicly available the main parameters used for targeting, including criteria used for excluding consumers.[1148] Such transparency may shed light on ways in which OBA can lead to significant effects, including consumer manipulation and discrimination.

[1141] *See Id*. *See also* CHEN, *supra* note 947 at 122–123.

[1142] C/13/687315 / HA RK 20-207, *Uber ADM*, Rechtbank Amsterdam (2023) ECLI:NL:GHAMS:2023:796.

[1143] Case C-634/21, Schufa Holding and Others (Scoring), Request for a preliminary ruling, 2021.

[1144] Andreas Hauselmann, *supra* note 1140.

[1145] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 1119.

[1146] *Id.*

[1147] *Id.*

[1148] Digital Services Act, *supra* note 2, art. 39(2)(e).

Lastly, applying Article 22 GDPR to OBA suggests that the practice can only be legitimized by "explicit" consent.[1149] Such a higher standard of consent usually consists of a written statement or a signature of the consumer revealing the explicit desire of the consumer to be subjected to such processing, but it can also include signing a form, electronic signature, or two-step verification.[1150] Explicit consent serves the purpose of clearing any doubt that the consumer wishes to accept such data processing.[1151]

6.2.4. The Prohibition of Unfair Practices and OBA

The Unfair Commercial Practices Directive (UCPD) provides a final filter for evaluating boundaries of consumer manipulation via OBA.[1152] The UCPD prohibits unfair practices that "materially distort" consumer behavior in the context of their "transactional decisions," including in the context of OBA when consumers consent to OBA, continue scrolling the feed, or click an advertisement.[1153] Article 2(e) UCPD explains that material distortion means "appreciably impairing the consumer's ability to make an informed decision".[1154] In light of the theory of influence developed in Chapter 3, material distortion is equal to exploiting consumer decision-making vulnerability through manipulation or coercion. Manipulative practices of OBA can be regarded as "unfair" and violate the UCPD in *five* different ways (section 6.1.1): if the practice is (1) on a blacklist, (2) a misleading omission, (3) a misleading action, (4) an aggressive action, or (5) failing the general test.[1155]

First, the UCPD blacklist provides limited guidance in consumer manipulation via OBA. Item 11 of Annex I of the UCPD prohibits hidden advertorials or "using editorial content in the media to promote a product" without clearly disclosing paid advertisement.[1156] The UCPD requires an active disclosure of advertorials, without which a practice can be conceptualized as a misleading omission and thus prohibited (*MAP1: hidden advertorials*).[1157] Item 28 of Annex I UCPD prohibits "a direct exhortation to children" to buy products or persuade their parents in an advertisement that is regarded as aggressive practice. Although it has a broader

[1149] General Data Protection Regulation, *supra* note 44, art 22.

[1150] *Id.,* art. 9(2).

[1151] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Consent Under Regulation 2016/679* (2018).

[1152] European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 70.

[1153] *Commission Notice, Guidance on the Interpretation and Application of Directive 2011/83/EU of the European Parliament and of the Council on Consumer Rights*, O.J. 2021 (C 525) 1, 2.4 (2021) [hereinafter Guidance on the Interpretation of the Unfair Commercial Practices Directive].

[1154] Unfair Commercial Practices Directive, *supra* note 42, art. 2(e).

[1155] *See* Zard and Sears, *supra* note 1, 841.

[1156] Unfair Commercial Practices Directive, *supra* note 42, an. I, art. 11.

[1157] *Id.,* an. I, art. 11.

scope than OBA, such a prohibition further re-iterates the prohibition of OBA targeted for children (*MAP15*: *targeting children*).

Second, Article 7 UCPD prohibits the *misleading* omission or provision of "material" information consumers need to make transactional decisions (e.g., consent to OBA, click an ad).[1158] Until the DSA, there was limited guidance on what constituted "material information" in the context of OBA.[1159] This could be, for instance, failing to identify commercial intent (e.g., *MEP1: free-framing*).[1160] The introduction of the online advertising transparency requirements of the DSA sheds more light: Article 26 (1) DSA requires "online platforms" to disclose the commercial intent, identity of advertisers, and targeting criteria of each advertisement (subsection 6.1.4.2).[1161] While the requirement is limited to "online platforms", it also guides other digital service providers on what information can be regarded as material in the context of OBA. This thesis argues that such non-disclosure by any digital service provider would amount to a violation of Article 7 UCDP.[1162]

Thirdly, Article 6 UCPD also prohibits provision of misleading information or active deception.[1163] In the context of OBA, misleading actions may include disclosing false targeting criteria but also providing false hierarchies and misdirection when offering consumers consent to OBA. Within the theory of influence developed in this thesis, misleading omission (Article 7 UCPD) and action (Article 6 UCPD) fall under the forms of manipulation that exploit the decision-making vulnerability of imperfect information. It is evident that the UCPD covers practices often referred to as "dark patterns," including in the context of OBA.[1164] Note that Article 25 (1) DSA prohibits "online platforms" from designing online interfaces that deceive and manipulate.[1165] However, the Article 25 (1) DSA prohibition does not apply to dark patterns directed to consumers in the context of OBA – Article 25(2) DSA excludes application of the prohibition from cases that are covered by the UCPD and the GDPR, in which consumer manipulation via OBA

[1158] *Id.,* art. 7.

[1159] *See also* Zard and Sears, *supra* note 1, 841-942.

[1160] *See* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.9.2.

[1161] Digital Services Act, *supra* note 2, art. 26(1).

[1162] It is recommended that the Article 26(1) DSA requirements are added to Annex II UCPD.

[1163] Unfair Commercial Practices Directive, *supra* note 42, art. 6. ("A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise.")

[1164] *See* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.9.2.

[1165] Digital Services Act, *supra* note 2, art. 25, rec 67.

falls in. Nevertheless, Article 25(2) DSA reveals what types of interface design patterns can be considered misleading under Article 7 UCPD.

Fourthly, Articles 8-9 UCPD prohibit "aggressive practices" that "significantly impair consumer's freedom of choice".[1166] In light of the theory of influence developed in this thesis, aggressive practices can be regarded as forms of coercion in case the influence is overt (e.g., physical force) or manipulation in case the influence is covert (e.g., hidden exploitation of biases). Article 9 (c) UCPD explains that aggressive practices may involve "exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgment."[1167] This is often understood as "undue influence".[1168] Article 2(j) UCPD defines "undue influence" to mean "exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision."[1169] Targeting to (or disregarding that an algorithm is likely to target to) exploit consumers' decision-making vulnerabilities can amount to exerting undue influence.[1170]

With this in mind, manipulative extraction practices (MEPs) 12-13 and manipulative advertising practices (MAPs) 8-17 that are targeted to or, in effect, exploit consumer decision-making vulnerabilities can be considered to such undue influence. Note that while undue influence covers consumer manipulation via OBA, it is broader and also covers instances in which overt forms of influence are likely to exploit consumer vulnerabilities. For example, Meta's adoption of a transparency mechanism of targeting criteria in 2021 revealed that in Denmark, payday loans targeted people interested in gambling.[1171] This can be considered exploitative under the theory of influence developed in this thesis and was found to be undue influence, thus aggressive practice by the Danish consumer ombudsman.[1172]

Fifthly, Article 5 (2) UCPD provides the general prohibition of unfair practices.[1173] Article 5(2) UCPD acts as the safety net for prohibiting commercial practices that materially distort consumer behavior and "are contrary to professional diligence".[1174] The concept of professional diligence is sometimes referred to as the

[1166] Unfair Commercial Practices Directive, *supra* note 42, art. 8.

[1167] *Id.*, art. 9(c).

[1168] *See* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.10.

[1169] Unfair Commercial Practices Directive, *supra* note 42, art. 2(j).

[1170] *See* GALLI, *supra* note 41, at 238–40. *See also* Hacker, *supra* note 54.

[1171] *See* TRZASKOWSKI, *supra* note 41, 246.

[1172] *Id.* 246.

[1173] *See* Unfair Commercial Practices Directive, *supra* note 42, art. 5(2).

[1174] *See Id.*, art. 5(2).

criterion of "honest market practices" and the principle of "good faith".[1175] In other words, acting in accordance with the requirements of professional diligence may mean that digital service providers comply with the codes of conduct.[1176] It can also mean to comply with the requirements prescribed by other legislative documents, such as the GDPR.[1177] As Article 39 DSA and Article 69 EC.AIA (section 6.1.4.3) introduce codes of conduct relevant to the OBA industry, Article 5(2) UCPD can act as a potent tool for setting boundaries for consumer manipulation via OBA.

In sum, the UCPD can be interpreted to capture consumer manipulation via OBA entirely. While the UCPD may be substantively sufficient to safeguard consumer manipulation harms of OBA, its enforcement is associated with three pressing challenges: (1) the UCPD can only be used to classify practices as unfair *ex-post* (except blacklisted practices); (2) enforcing the UCPD to halt consumer manipulation via OBA, would require interpretation of digital consumer as more than ordinarily vulnerable; and (3) the UCPD enforcement needs to focus beyond economic harms.

Firstly, the UCPD is a consumer-complaint tool that requires post-factum evaluation of particular practices to classify them as unfair.[1178] In the *Orange Polska* case, the CJEU interpreted that practices cannot be classified as aggressive unless "a factual and case-specific assessment of its features has been carried out in the light of the criteria set out in Articles 8 and 9."[1179] Therefore, while it seems that the UCPD prohibits all manipulative practices of OBA, operationalizing this would mean "a factual" and "case-specific" evaluation of each practice. As manipulative practices are hidden by nature, and consumers lack awareness of how they exploit vulnerabilities, UCPD has had limited use. Implementation of the DSA is likely to change this. By providing advertising transparency rules in Article 26(1) DSA and VLOP/VLOSE advertising repository rules in Article 39 DSA, the DSA is creating the visibility necessary to operationalize the UCDP concerning manipulative practices.[1180]

Secondly, under the UCDP, consumers are not protected from *every* commercial practice that can potentially exploit their vulnerability.[1181] Instead, the UCDP prohibits commercial practices that are likely to exploit the decision-making of an "average consumer" who is "reasonably well informed and reasonably

[1175] GALLI, *supra* note 41, 248.

[1176] *See* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.7.

[1177] *See* Hacker, *supra* note 54, 12.

[1178] *See* Laux, Wachter & Mittelstadt, *supra* note 321, 740.

[1179] Case C-628/17, *Orange Polska*, 12 June 2019 ECLI:EU:C:2019:480. (2019).

[1180] *See also* GALLI, *supra* note 41, 248.

[1181] *See* Zard and Sears, *supra* note 1.

observant and circumspect" (section 6.1.1).[1182] For example, *Puffery* or boastful exaggeration can exploit *some* consumers but is expected to be identified as such by an average consumer and thus is considered fair play in advertising.[1183] In case commercial practices are targeted, the UCPD provides two additional variations of the benchmark: "average targeted consumer" refers to the average member of the targeted audience (Article 5(2)(b) UCPD),[1184] and "targeted vulnerable consumer" to the average member of the group that is considered vulnerable due to their group characteristics, such as mental or physical infirmity, age, or credulity (Article 5(3) UCPD).[1185]

Recital 19 UCPD suggests that commercial practice targeting vulnerable consumers can be considered unfair if vulnerability exploitation is foreseeable.[1186] Such understanding ideally matches the theory of influence developed in this thesis (section 3.3.3). The European Commission has clarified that consumer vulnerability is not limited to the labeled groups referred to in Article 5(3) UCPD but includes layers of vulnerability, as explained in this thesis (section 3.3.2).[1187] These three variations of the "average consumer" benchmark provide a perfectly sufficient way to capture the vulnerability of the digital consumer and thus set the boundary of consumer manipulation via OBA.[1188] Nevertheless, the UCDP clarifies that the "average consumer" benchmark is not a statistical test.[1189] This means that the national authorities and the courts depend on exercising their own judgment to

[1182] *See* Unfair Commercial Practices Directive, *supra* note 42, rec. 18. *See also* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.5. ("In the case-law of the Court, the average consumer is a reasonably critical person, conscious and circumspect in his or her market behaviour.")

[1183] *See* Laux, Wachter & Mittelstadt, *supra* note 321, 740. Note that within the theory of influence "puffery" targeted to average consumer would be considered to be "manipulative". *See also* Cristopher Decker, *Concepts of the Consumer in Competition, Regulatory, and Consumer Protection Policies*, 13 J. COMP. L. & ECON. 151, 184 (2017).

[1184] Unfair Commercial Practices Directive, *supra* note 44, art.5, rec 18.

[1185] *Id.*, art. 5(3), rec.19.

[1186] *Id.*, art. 5(3), rec.19.

[1187] Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 2.5. ("The concept of vulnerability is not limited to the characteristics listed in Article 5(3), as it covers also context-dependent vulnerabilities. Multi-dimensional forms of vulnerability (146) are particularly acute in the digital environment, which is increasingly characterised by data collection on socio-demographic characteristics but also personal or psychological characteristics, such as interests, preferences, psychological profile and mood.") *See* DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, EUR. COMM'N, FACT SHEET: UNDERSTANDING CONSUMER VULNERABILITY IN THE EU'S KEY MARKETS (2016), https://ec.europa.eu/info/sites/default/files/consumer-vulnerability-factsheet_en.pdf.

[1188] *See* GALLI, *supra* note 41, at 181–205.

[1189] Unfair Commercial Practices Directive, *supra* note 44, art.5, rec 18.

evaluate if a particular commercial practice is likely to impair the decision-making of "average", "average targeted," and "targeted vulnerable" consumers.[1190]

While various scholars argue that the UCPD clearly regards digital consumers (also in the context of OBA) as more than ordinarily vulnerable, some still call for explicit recognition of "digital vulnerability" in legal texts.[1191] These calls reflect the significant weight the "average consumer" benchmark has in safeguarding against consumer exploitation in the digital world: recognition of the vulnerability of digital consumers is a pre-condition for classifying all manipulative practices of OBA as unfair under the UCPD. While there is no CJEU case law concerning digital vulnerability, the court is now considering the *Compass Banca* case (C-646/22-1), which will answer whether consumers must be regarded as universally vulnerable.[1192]

Thirdly, and lastly, Article 1 UCPD clarifies that the UCPD only protects against economic harms.[1193] Typically, the UCPD does not safeguard against health, safety, affinity, or environmental harms of business-to-consumer (B2C) commercial practices.[1194] However, the CJEU has clarified that the UCPD safeguards other interests in case they are in conjunction with the consumer's economic interest.[1195] This "economic" aspect of the UCPD was considered a limiting factor in enforcing consumer protection rules for OBA, as some argued that economic exchange was absent in OBA contracts.[1196] Over time, consumer protection authorities, such as those in Germany[1197] and Italy,[1198] have clarified that consumer protection rules

[1190] *Id.*, rec. 18. Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1155 at 2.5. ("In the case-law of the Court, the average consumer is a reasonably critical person, conscious and circumspect in his or her market behaviour.")

[1191] *See generally* Natali Helberger, Marijn Sax, Joanna Strycharz & Hans-Wolfgang Micklitz, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, 45 J. CONSUMER POL'Y 175, 175 (2022). *See* Laux, Wachter & Mittelstadt, *supra* note 321. *See* GALLI, *supra* note 35, at 188–92. *See* TRZASKOWSKI, *supra* note 35 at 115-120. *See* HELBERGER ET AL., *supra* note 461.

[1192] *Case C-646/22*, Compas Banca Request, *supra* note 434.

[1193] Unfair Commercial Practices Directive, *supra* note 44, art.1.

[1194] *See* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 1.1.1.

[1195] Case C-540/08, *Mediaprint Zeitungs- und Zeitschriftenverlag*, October 9, 2010. ECLI:EU:C:2010:660. *See also* Guidance on the Interpretation of Unfair Commercial Practices Directive, *supra* note 1153, 1.1.1.

[1196] *See e.g.,* Helberger, Zuiderveen Borgesius & Reyna, *supra* note 42, at 3, 8.

[1197] In its analysis German court argued that a contractual relationship is present as Facebook user gave their personal data in exchange of the online platform's services. *See* Kammergericht Berlin [KG][Higher Court of Berlin] Jan. 24, 2014, 5 U 42/12 at section B.2.bb (Ger.) Moreover, the German regional court prohibits Apple to require its users to accept sharing personal data to third parties in order to receive Apple services. *See* Landgericht Berlin [LB] [Regional Court of Berlin] Apr. 30, 2013, 15 O 92/12 (Ger.).

[1198] Italian Consumer Market Authority, and then Administrative Court of Appeal concluded that Facebook's slogan "it is free and it will always be free" is misleading, as consumers are providing

apply in situations when consumers provide their monetizable attention and data in exchange for receiving digital services. The Digital Content Directive (DCD) harmonized such interpretation across the EU.

Nevertheless, it seems that UCPD safeguards market, environment, affinity, privacy, integrity, and dignity harms of consumer manipulation via OBA only in case these harms occur in conjunction with the economic harms of the consumer. It can also be argued that loss of time, occurring in all consumer manipulation via OBA, can be understood as economic harm (e.g., loss of wages), and thus, all consumer manipulation harms of OBA can be considered captured by the UCPD. Such understanding, while theoretically plausible, is not a straightforward route. Thus, consumer manipulation via OBA continues to be primarily addressed via enforcement of the GDPR.[1199]

6.2.5. The Proposed Prohibitions of Manipulation via AI

The European Commission's proposed Artificial Intelligence Act (AIA) includes two prohibitions that are particularly relevant to consumer manipulation via OBA. Table 6-1 below provides the text of these prohibitions and amendments proposed by the European Parliament (EP.AIA) and the Council (C.AIA).[1200]

Table 6-1. Article 5(1)(a)-(b) EC.AIA, EP.AIA and C.AIA (by Author)

5(1)	Proposal (EC.AIA)	Parliament Mandate (EP.AIA)	Council Mandate (C.AIA)
(a)	the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;	the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness ~~in order to~~ or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision they would not have taken otherwise in a	the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness ~~in order to~~ with the objective to or the effect of materially distorting a person's behaviour in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm;

personal data in exchange of receiving Facebook's services. L'Autorita Graante Della Concorrenza e Del Mercato [AGCM] [Consumer Market Authority] Nov. 29, 2018, Provvedimento n.27432 (It.) [hereinafter AGCM]; *see also* Marta Bianchi, *T.A.R., Facebook Case: Personal Data as Contractual Consideration. Antitrust Procedure Initiated [Tar Lazio 10 January 2020, n.ri 260 and 261]*, DIRITTO DI INTERNET (Feb. 13, 2020).

[1199] European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53.

[1200] *See* AI Act Mandates, *supra* note 367, ¶181, 182.

		manner that causes or is likely to cause that person another person ~~physical or psychological~~, or group of persons significant harm.	
(b)	the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;	the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a person or a specific group of persons, including characteristics of such individual's or group of persons' known or predicted personality traits or social or economic situation, ~~due to their~~ age, physical or mental ability, ~~in order to~~with the objective or to the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is likely to cause that person or another person ~~physical or psychological~~ significant harm;	the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, ~~physical or mental disability, in order to~~ disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm;

The EC.AIA is grounded in the terminology of the UCPD.[1201] These prohibitions are intended to expand the UCPD protections to non-economic situations and also when manipulation leads to non-economic harms.[1202] Article 5(1)(a) EC.AIA seems to prohibit manipulative AI practices that are "subliminal".[1203] Article 5(1)(b)EC.AIA prohibits AI practices that exploit vulnerabilities.[1204] The distinction between these two forms of autonomy violation is somewhat similar to the distinction between "misleading" and "aggressive" practices in the UCPD. Still, "subliminal" influence may not be an appropriate framing.[1205] In essence, Article 5(1)(a) EC.AIA can be understood to focus on *hidden* influence "beyond a person's consciousness".[1206] Indeed, Article 5(1)(a) EP.AIA reveals the legislator's intention to regulate "purposefully manipulative or deceptive techniques".[1207] In contrast, Article 5(1)(b) EC.AIA can be understood to

[1201] Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 99 (2021) https://osf.io/preprints/socarxiv/38p5f/ (last visited May 8, 2023).

[1202] *Id.*

[1203] AI Act Proposal, *supra* note 52 art. 5(1)(a).

[1204] *Id.* art. 5(1)(b).

[1205] *See* Veale and Zuiderveen Borgesius, *supra* note 1203, 99.

[1206] *See* AI Act Proposal, *supra* note 52 art. 5(1)(a).

[1207] *See* AI Act Mandates, *supra* note 367, ¶181, 182.

cover situations in which an AI system can exploit a person's vulnerability, both covertly (manipulation) or overtly (coercion).

Understood this way, a combination of Article 5(1)(a) and Article 5(1)(b) AIA prohibitions can potentially cover instances of manipulation via OBA when consumers are targeted algorithmically (e.g., MAPs 8-17). Nevertheless, versions of Article 5(1)(a)-(b) AIA have three shortcomings in addressing consumer manipulation harms of OBA.

Firstly, Article 5(1)(a)-(b) EC.AIA implies the deliberative intentionality of manipulation via AI systems. In light of the theory of manipulation constructed in Chapter 3 and Chapter 4 of this thesis, digital service providers can be said to manipulate consumers via OBA when they intend to influence a consumer towards a particular action (e.g., clicking an ad), but they disregard that their AI systems are likely to exploit consumer vulnerabilities. Both EP.AIA and C.AIA seem to successfully address this shortcoming, clarifying that prohibition applies to AI systems "with the objective or to the effect of" exploiting a person.[1208] Nevertheless, the European Parliament's reference to "purposefully manipulative" practices raises further questions.

Secondly, Article (5)(1)(a)-(b) EC.AIA safeguards against *physical* and *psychological* harms, conceptualized as "integrity" harms in Chapter 5. Such framing of harms may leave a variety of consumer manipulation harms of OBA unaddressed. EP.AIA and C.AIA seem to resolve this shortcoming by reframing prohibition to cover manipulative AI practices that cause "significant" harm to a person or group of persons.[1209] This can address the societal harms of consumer manipulation via OBA, such as conceptualized in section 5.2.7. However, EP.AIA only partially resolves shortcomings in Article 5(1)(b) EC.AIA, where the threshold of harm is also that it is *significant*, but it is only limited to persons (not group of persons and society).

Thirdly, and lastly, Article (5)(1)(b) EC.AIA considers the "labeled" or "group" concept of vulnerability, referring to age and physical or mental disability. EP.AIA reframes this norm to include a layered concept oif vulnerability stemming from people's inherent traits (e.g., personality) or economic and social situations. C.AIA expands EC.AIA by only adding economic and social situations as additional layers of vulnerability that seems limited conceptualization (compared to EP.AIA)

In sum, Article (5)(1)(a)-(b) AIA in combination can be understood to cover manipulative practices of OBA that rely on algorithmic systems. OBA often relies on AI, for example, when targeting occurs through the "lookalike audiences" feature (section 4.3.2). This thesis argues that EP.AIA amendments make Article 5(1) AIA to be operationalizable in the context of OBA. Nevertheless, removing the condition of "purposefulness" of manipulative influence in Article 5(1)(a) EP.AIA and adding

[1208] *Id.*
[1209] *Id.*

harms to "groups of persons" in Article 5(1)(b) EP.AIA can provide further clarity about the boundaries of consumer manipulation via OBA when it relies on AI systems.

6.3. Legal Grounds for OBA

OBA relies on data, such as consumer's Web browsing history or their on-platform behavior (e.g., clicks, likes), that in the EU qualifies as "personal data" because it relates to an identified or identifiable individual (section 2.2.2).[1210] Therefore, all digital service providers that want to engage in OBA in the EU must comply with the GDPR, which regards the processing of personal data as prohibited *unless* service providers demonstrate they meet the legal grounds prescribed in Article 6(1) GDPR.[1211]

In practice, digital service providers have relied on three legal bases for OBA, which are analyzed in the three sections below: section 6.3.1 analyzes consumer's consent requirement under Article 6(1)(a) GDPR as a legal basis for OBA, section 6.3.2 analyzes the validity of processing OBA data because it "is necessary for the performance of a contract" under Article 6(1)(b) GDPR, and section 6.3.3 analyzes the validity of processing OBA data due to "legitimate interest" of publishers to engage in OBA under Article 6(1)(f) GDPR.

6.3.1. Consent

Article 8(2) CFREU explicitly mentions a person's consent as one of the legal basis for processing personal data about them.[1212] Article 6(1)(a) GDPR reiterates this and is typically understood as the *only* valid legal basis to process personal data for OBA.[1213] Nevertheless, as the GDPR's consent requirements are challenging to meet, some digital service providers avoid using this legal basis for processing data for OBA. Section 6.3.1.1 addresses the conditions that must be met for consent to be regarded as valid. Section 6.3.1.2 elaborates on particular challenges for the validity of consumer consent in AdTech. Section 6.3.1.3 describes the nature of the contractual relationship between digital service providers and consumers upon consumer consenting to OBA.

[1210] *See* Frederik J. Zuiderveen Borgesius, *Personal Data Processing for Behavioural Targeting: Which Legal Basis?*, 5 INT. DATA PRIV. L. (2015).

[1211] General Data Protection Regulation, *supra* note 44, art. 6(1).

[1212] CFREU, *supra* note 45, art. 8(2).

[1213] *See* Zuiderveen Borgesius, *supra* note 1212.

6.3.1.1 Conditions

Acquiring legally valid consent is not a trivial task.[1214] Consent is the genuine expression of consumer autonomy, which can waive the human rights level prohibition against the processing of their personal data.[1215] Article 4(11) GDPR defines consent as a "freely given, specific, informed, and unambiguous indication" of a consumer's wishes that is disclosed "by a statement or an explicit affirmative action that signifies an agreement to the processing of personal data".[1216] In essence, the GDPR aims to ensure consumers give consent without manipulative and coercive influence.[1217] Typically, determining the validity of consent requires evaluating whether consent is (i) informed, (ii) specific, (iii) unambiguous, and (iv) freely given.[1218]

Firstly, *informed* consent means that digital service providers processing consumer personal data must disclose at least their identity and the purpose of processing activity (e.g., personalized advertising).[1219] Such disclosure must provide consumers with a substantial understanding of what they agree to.[1220] Article 7 GDPR clarifies that consent transparency entails more than mere information provision and that information should be provided in "intelligible and easily accessible form, using plain language".[1221] For example, the French Data Protection Authority (DPA) has found that Alphabet violated requirements of "informed" consent in the context of OBA, as it provided information about purposes of processing in a "generic and vague manner".[1222] This criterion can be considered violated if insufficient or inaccurate information is provided.[1223] It can be argued that in the context of OBA, substantial understanding can only be ensured if digital

[1214] *See* detailed overview on GDPR's consent requirements for OBA in CHEN, *supra* note 947 at 113–120.

[1215] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 58.

[1216] General Data Protection Regulation, *supra* note 44, art. 4 (11). ("'[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.")

[1217] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 58-73.

[1218] *See* Schermer, Custers, and van der Hof, *supra* note 888, at 3. *See also* Veale and Zuiderveen Borgesius, *supra* note 31, at 236.

[1219] General Data Protection Regulation, *supra* note 44, recs. 42, 32, 58.

[1220] *See* Schermer, Custers, and van der Hof, *supra* note 888, at 3.

[1221] General Data Protection Regulation, *supra* note 44, art. 7, rec. 58.

[1222] *See The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, EUROPEAN DATA PROTECTION BOARD (2019), https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (last visited May 3, 2023).

[1223] *See* Schermer, Custers, and van der Hof, *supra* note 888, at 3.

service providers convey information regarding the potential risks of agreeing to OBA (e.g., OBA may lead to harm to integrity).[1224]

Secondly, consent must be *specific* or authorize a particular course of action.[1225] This criterion requires digital service providers to ask consumers to consent to each processing activity if they undertake multiple processing operations (e.g., personalized feed and advertising).[1226] For instance, the Norwegian DPA has found Grindr to violate the condition for "specific" consent because the dating app asked for consent to OBA in a request bundled with the acceptance of the general privacy policy.[1227] The specificity criterion is closely related to the criterion of informed consent, which aims to ensure that consumers are sure of what they are consenting to.[1228] These criteria are particularly relevant in the context of OBA within gatekeeper ad networks and in AdTech, where various third parties are involved (section 6.3.1.2).[1229]

In the context of the designated gatekeepers, such as Alphabet and Meta, the DMA has clarified the requirement of specific consent in two provisions: Article 5(2)(a) DMA prohibits gatekeepers from processing consumer data for OBA that is collected by third parties (e.g., online newspapers, online games) that are part of their advertising networks (e.g., Google Display Network, Meta Audience Network) unless the consumer consents that the gatekeeper combines data from each third party.[1230] Article 5(2)(b) DMA prohibits gatekeepers from combining consumer data between their different platform services (e.g., between Instagram and Facebook) unless the consumer consents to each processing activity separately.[1231]

Thirdly, consent has to be an *unambiguous* indication of the consumer's wishes.[1232] This refers to the requirement that consent cannot be implied by, for

[1224] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 60. Disclosure of risk has been explicitly required in the now-stalled proposed ePrivacy Regulation. *See* ePrivacy Regulation, *supra* note 43 at rec. 24. ("Information provided [...] should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites(third) party cookies are always or never allowed.")

[1225] *See* Schermer, Custers, and van der Hof, *supra* note 88, at 5.

[1226] General Data Protection Regulation, *supra* note 44, rec. 32.

[1227] Norwegian Data Protection Authority (Datatilsynet) Administrative Fine - Grinder LLC Offl. § 13 jf. fvl. § 13 (1) nr. 2 (Dec. 13, 2021) (No.).

[1228] *See* Schermer, Custers, and van der Hof, *supra* note 888, 5.

[1229] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 58.

[1230] Digital Markets Act, *supra* note 14, art.5(2)(a).

[1231] *Id.*

[1232] General Data Protection Regulation, *supra* note 44, art. 4 (11).

instance, because consumers access the website of the digital service provider.[1233] In other words, there has to be no doubt that the consumer consented to data processing.[1234] In case OBA is considered to have significant effects and fall under the scope of Article 22 GDPR (section 6.2.3), consent not only has to be unambiguous but also "explicit", suggesting a higher level of responsibility for digital service providers.[1235] Explicit consent can be expressed by filling out the consent form or electronic signature.[1236]

Fourthly, consent has to be *freely given* and, therefore, an expression of a consumer's genuine desire.[1237] Digital service providers have to ensure that the decision-making of the consumer is free of coercive and manipulative influences.[1238] Article 7 GPDR lists two such elements to consider when evaluating if consent is freely given – (a) whether publishers provide alternative options[1239] and (b) whether there is an "imbalance" between parties.[1240] These two elements can help evaluate the legitimacy of the OBA industry's consent practices.

Firstly, the most essential criterion in determining the freeness of consent is that the provision of digital services is not dependent on consumers consenting to OBA.[1241] As the GDPR enforcement has demonstrated that consumer consent is the only legal basis for OBA (sections 6.3.2 and 6.3.3), publishers are increasingly moving towards the "OBA-or-Pay" model in which they monetize their digital services either by OBA or by subscription fees.[1242] However, significant legal uncertainty exists about whether consumer consent can be regarded as freely given within the OBA-or-Pay model.[1243] The German DPA has ruled such a model to be coercive and, thus, illegal in the context of online newspapers.[1244] In contrast, the French DPA found that the OBA-or-Pay model *can* be legitimate if case-by-case assessment reveals that the alternative is fair (e.g., is provided for a reasonable

[1233] *See* Schermer, Custers, and van der Hof, *supra* note 888, at 5.

[1234] *See Id.*, at 7.

[1235] General Data Protection Regulation, *supra* note 44 art. 9(2).

[1236] *See* Schermer, Custers, and van der Hof, *supra* note 888, at 5.

[1237] General Data Protection Regulation, *supra* note 44, rec. 32.

[1238] *See* Veale and Zuiderveen Borgesius, *supra* note 31 at 236. *See generally* Schermer, Custers, and van der Hof, *supra* note 888.

[1239] *See* General Data Protection Regulation, *supra* note 44, art. 7 (4). *See* EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on Consent under Regulation 2016/679*, 8 (2020).

[1240] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 63.

[1241] *See Id.*, at 67.

[1242] *See generally* Morel et al., *supra* note 546.

[1243] *See Id.*

[1244] Data Protection of Lower Saxony (Die Pandesbeauftragte für den datenschutz niedersachsen), Decision regarding der Standard. Tech. rep. (May, 17, 2023) (Ger.), https://noyb.eu/sites/default/files/2023-07/11VerwarnungPurAboModellfinalgeschwrztp_Redacted.pdf (last visited Oct 19, 2023).

price).[1245] It seems that the Austrian and the Spanish DPAs do not find the OBA-or-Pay model necessarily illegitimate.[1246]

Secondly, an increasingly accepted interpretation is that the imbalance between the parties can be established when publishers hold significant market power.[1247] In the *Meta v. Bundeskartellamt* case, the CJEU acknowledged that Meta's dominant position in the social network market was essential for determining consumer consent's freeness.[1248] Such imbalance between parties can be considered one of the elements in evaluating the freeness of consent, including in the OBA-or-Pay model. Therefore, while it is likely that this model can be allowed if case-by-case evaluation deems it fair and free of manipulative and coercive influence, coming to such a conclusion can be complicated if the consumer is consenting to publishers with significant market power, particularly gatekeepers. The DMA solidifies this paradigm by requiring gatekeepers to ask consumers to consent for OBA and also to offer an "equivalent" and possibly "less personalized alternative" of their platforms that is not of "degraded quality".[1249]

In the light of the theory of influence developed in section 3.3.3 of this thesis, consent acquired by the gatekeeper through the "OBA-or-Pay" model is coercive and cannot be freely given no matter how "reasonable" the price of the non-OBA model is (section 4.1.3). This argument stems from a position of "heightened vulnerability" for the consumers of gatekeepers, stemming from relational dependency. For example, online newspaper publishing is a highly competitive market, and in case a consumer is not happy with the "OBA-or-Pay" option, they are likely to find a news source that either costs less or involves processing less data. In contrast, this thesis argues that consumers accessing gatekeeper platforms (e.g., YouTube, Instagram) cannot be considered to have an actual choice and thus express a genuine preference for OBA in the "OBA-or-Pay" model.

Regardless, Meta is considering launching the "OBA-or-Pay" model for Facebook and Instagram.[1250] The company justifies this model by referring to the CJEU judgment in the *Meta v. Bundeskartellamt* case, where the court mentioned the possibility that Meta could provide a subscription-based alternative of its

[1245] *See Cookie walls : la CNIL publie des premiers critères d'évaluation*, CNIL (2022), https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation (last visited Oct 19, 2023).

[1246] *See generally* Morel et al., *supra* note 546. *See* Austria challenges EU newspapers' pay-or-cookie walls, EURACTIV (2023), https://www.euractiv.com/section/media/news/austria-challenges-eu-newspapers-pay-or-cookie-walls/ (last visited Jun 1, 2023).

[1247] EUROPEAN DATA PROTECTION BOARD, *supra* note 1241 at 8.

[1248] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017.

[1249] Digital Markets Act, *supra* note 14, recs. 36-37.

[1250] *See* Sam Schechner, *Meta Plans to Charge $14 a Month for Ad-Free Instagram or Facebook*, WALL STREET JOURNAL, Oct. 3, 2023, https://www.wsj.com/tech/meta-floats-charging-14-a-month-for-ad-free-instagram-or-facebook-5dbaf4d5 (last visited Oct 18, 2023).

services.[1251] However, this thesis argues that the CJEU's reference to such an alternative is misinterpreted. In the *Meta v. Bundeskartellamt* case, The CJEU does not consider the validity of consent within the "OBA-or-Pay" model, but rather, the validity of the contract that involves processing OBA data which is not necessary for the contract in question.[1252] The court finds that consumers must be able to reject the processing of such OBA data that is not necessary for the contract and still receive the services of the social network, "if necessary for an appropriate fee".[1253]

Indeed, nothing prohibits Meta from offering Facebook and Instagram solely via a subscription model for an appropriate fee. Nevertheless, if Meta also offers an OBA-funded alternative to these platforms in addition to the subscription model, consent validity to this alternative must be evaluated independently. As argued in the previous paragraphs, consent to OBA under such an "OBA-or-Pay" model would be invalid. This suggests that in case gatekeepers have to provide the third alternative, similar to OBA, which does not require monetary payment and, similar to the subscription model, does not require processing of behavioral data.

The DMA would still require that such a free alternative in the "Free-OBA-Pay" model is also "equivalent" and not of "degraded quality".[1254] The gatekeepers can monetize such a free alternative by selling contextual or broad demographic advertising that does not involve tracking and predicting consumer behavior. Recital 37 DMA also clarifies that gatekeepers must design their online interfaces in a way that does not coerce or manipulate consumers and ensure that giving consent (also for OBA) is as easy as withdrawing it.[1255] This may suggest that gatekeepers have to introduce a button or toggle that allows consumers to withdraw consent for OBA or alternate between "Free-OBA" options.

Lastly, consent to OBA is not automatically validated if the consumer agrees to the personal data processing by publishers that are not gatekeepers. Instead, the validity of such consent has to be evaluated on a case-by-case basis and requires the conclusion that the consumer is free of manipulative and coercive influence.

6.3.1.2 Consent in AdTech

Acquiring informed, specific, unambiguous, and free consent is more complicated in case OBA takes place in the open display advertising exchange or in

[1251] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017, 150. ("Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.")

[1252] *Id.*

[1253] *Id.*

[1254] Digital Markets Act, *supra* note 14, recs. 36-37.

[1255] *Id.*

"AdTech". As explained in section 2.4.1, OBA in AdTech includes hundreds of "vendors" (industry term), including publishers, advertisers, and ad intermediaries competing for advertising space in the real-time bidding (RTB) auction. Most of the open exchange is supported by the *OpenRTB* protocol provided by the Interactive Advertising Bureau (IAB) and the *Authorized Buyers* protocol provided by Alphabet. By December 2023, all vendors using both protocols are expected to implement "Transparency & Consent Framework (TCF) 2.2." provided by IAB Europe.[1256]

TCF 2.2. emerged in response to the decision of the Belgian DPA that, in February 2022, found the earlier versions of TCF to violate the GDPR.[1257] On 25 April 2018, a month before the GDPR went into force, IAB Europe adopted an early version of TCF in order to help OpenRTB vendors engage in OBA.[1258] Consent management platforms (CMPs) that emerged to facilitate earlier versions of TCF provided standardized cookie banners that collected consumers' cookie preferences in the "Transparency and Consent String" and shared them with all TCF participants.[1259] These versions of TCF entailed collecting consent for placing third-party cookies to comply with Article 5(2) ePrivacy Directive.[1260] As for processing data collected via these cookies for the purpose of OBA, early versions of TCF relied on legitimate interest prescribed in Article 6 (1)(f) GDPR.[1261] Therefore, when consumers accepted cookies on CMPs supporting early versions of TCF, they enabled hundreds and sometimes over a thousand unknown vendors to track and target them for OBA.[1262]

The Belgian DPA found that such reliance on Article 6(1)(f) GDPR by these third-party vendors violated the GDPR. The Belgian DPA also found that acceptance of cookies could not be considered valid consent according to Article 7

[1256] Kavya, *Google and IAB TCF v2.2: How Publishers Can Stay Ahead with CookieYes*, COOKIEYES (Jun. 2, 2023), https://www.cookieyes.com/blog/iab-tcf-cmp-for-publishers/ (last visited Oct 19, 2023).

[1257] *TCF 2.2 Launches! All You Need To Know*, IAB.EUROPE (May 16, 2023), https://iabeurope.eu/all-news/tcf-2-2-launches-all-you-need-to-know/ (last visited Oct 19, 2023). Note that IAB and IAB Europe are not the same organization.

[1258] *See* Veale and Zuiderveen Borgesius, *supra* note 31 at 230.

[1259] *See generally* Michael Veale, Midas Nouwens & Cristiana Santos, *Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?*, 2022 TECHNOL. REGUL. 12, 13–14 (2022).

[1260] ePrivacy Directive, *supra* note 43, art 5(3).

[1261] *See* Veale, Nouwens, and Santos, *supra* note 1261 at 13–14.

[1262] *See* Thea Felicity, *Top 5 Best Consent Management Platforms in 2022 To Easily and Legally Manage User Data*, TECHTIMES 5 (Aug. 3, 2022), https://www.techtimes.com/articles/272671/20220308/top-5-best-consent-management-platforms-in-2022-to-easily-and-legally-manage-user-data.htm (last visited Jan 5, 2023).

GDPR for TCF participants to process consumer data for OBA.[1263] The Belgian DPA argues that there are too many actors involved, and it would require disproportionate time for consumers to be meaningfully informed and understand whom they are consenting to and for what.[1264]

In September 2022, upon appeal of the IAB Europe, the Belgian DPA referred the case to the CJEU, requesting a preliminary ruling on this matter.[1265] While the CJEU judgment is not expected until 2024, the Belgian DPA requested IAB Europe to comply with the decision from July 11, 2023.[1266] As a response, on 16 May 2023, IAB Europe introduced TCF 2.2., which includes new rules for TCF participants.[1267] TCF 2.2. requires that the legal basis for OBA is consent from each of the "vendors". It seems that TCF 2.2. will significantly decrease the number of vendors publishers can allow to track their consumers. It also requires publishers to show the number of vendors on the first layer of banners where consumers can accept placing third-party cookies for OBA.

Indeed, by 2024, TCF 2.2. will be implemented by almost all participants in AdTech and will provide improved protections for consumers relative to its earliest versions. However, there is much skepticism as to what extent it can ensure compliance with Article 4, 6(1)(a), and 7 GDPR requirements of valid consent.[1268] One hesitation is regarding the criteria of the consent to be informed and specific. It is doubtful that consent can be considered specific if, by one click, consumers consent to numerous ad vendors whose identities they do not see even though they now see their number.[1269]

Therefore, it is likely that the industry requires a stronger consent mechanism than TCF 2.2., and as a result, OBA in AdTech will become more centralized, where only a few ad intermediaries track consumers on most of the Web. This process will take place in parallel with advancing "local" or browser-based advertising tools,

[1263] Belgian Data Protection Authority (Gegevensbeschermingsautoriteit), Decision on the merits 21/2022 of 2 February 2022: Complaint relating to Transparency & Consent Framework (DOS-2019-1377, 2 February 2022) (Be.).

[1264] *Id.*

[1265] Belgian Data Protection Authority (Gegevensbeschermingsautoriteit), *IAB Europe Case: The Market Court Refers Preliminary Questions to the Court of Justice of the EU*, (Jul. 9, 2022), https://www.dataprotectionauthority.be/citizen/iab-europe-case-the-market-court-refers-preliminary-questions-to-the-court-of-justice-of-the-eu (last visited Jan 5, 2023).

[1266] IAB Europe Seeks Court Decision on Validation Of The Action Plan as it Moves Forward With TCF Evolutions, IAB.EUROPE, https://iabeurope.eu/all-news/iab-europe-seeks-court-decision-on-validation-of-the-action-plan-as-it-moves-forward-with-tcf-evolutions/ (last visited May 4, 2023).

[1267] *TCF 2.2 Launches! All You Need To Know – IAB Europe*, *supra* note 1259.

[1268] *See e.g.,* Veale, Nouwens, and Santos, *supra* note 1261. *See e.g.,* Morel et al., *supra* note 546.

[1269] *See* Veale, Nouwens, and Santos, *supra* note 1261. *See also* Tim Cross, *IAB Removes Legitimate Interest from Reworked TCF*, VIDEOWEEK (May 16, 2023), https://videoweek.com/2023/05/16/iab-removes-legitimate-interest-from-reworked-tcf/ (last visited Jun 2, 2023).

such as those developed under Alphabet's Privacy Sandbox (section 2.4.3), that can further cement the power of gatekeepers in the OBA industry.

6.3.1.3 OBA Contracts

Traditionally, legal scholars have avoided framing consent to OBA as entering into a contract with a publisher.[1270] On the one hand, the protection of personal data is a fundamental right in the EU, and, therefore, it cannot be regarded as a commodity, such as money that can be traded in exchange for receiving digital services.[1271] On the other hand, the increasing prevalence within publishers to adopt the "OBA-or-Pay" model demonstrates that choosing to access digital services funded by OBA consumers enters into a ("data-for-access") bargain. Therefore, it would be counterintuitive to provide lesser protection for consumers when their economic bargain with the digital service provider also affects fundamental rights interests.[1272]

The Digital Content Directive (DCD) acknowledges data-for-access bargains between consumers and digital service providers and ensures that consumers of these "OBA contracts" are protected with contractual remedies.[1273] Article 3(1) DCD can be understood to apply only in situations when a consumer gives valid consent to the processing of personal data for OBA under Article 6(1)(a) and 7 GDPR. [1274] In other words, the bargain is not acknowledged when consumer personal data is processed because such processing is necessary to supply the digital content or comply with legal requirements (e.g., the obligation to identify users).[1275] The DCD clearly recognizes that the GDPR has primacy in evaluating the validity of consent in OBA contracts.[1276] It affirms that although personal data is not a

[1270] *See* Frederik Zuiderveen Borgesius, *Consent to Behavioural Targeting in European Law - What Are Policy Implications of Insights from Behavioural Economics?*, Amsterdam Law School Research Paper No.2013-43, 4 (2013).

[1271] *See* Gianclaudio Malgieri & Bart Custers, *Pricing Privacy – The Right to Know the Value of Your Personal Data*, 34 COMPUT. L. & SECUR. REV. 289 (2017).

[1272] The German and Italian authorities have affirmed that data-for-access bargain is an economic transaction to which consumer protection rules apply. *See* KG, 5 U 42/12 (Ger.), *supra* note 1197. *See also* AGCM, Provvedimento n.27432 (It.), *supra* note 1198.

[1273] *See* Digital Content Directive, *supra* note 940, rec. 24. ("Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies.")

[1274] Digital Content Directive, *supra* note 940, art. 3, rec. 24.

[1275] *Id. See also Commission Notice, Guidance on the Interpretation and Application of Directive 2011/83/EU of the European Parliament and of the Council on Consumer Rights*, O.J. 2021 (C 525) 1, 13.

[1276] *See* Digital Content Directive, *supra* note 940, rec. 24.

commodity, if the consumer consents to an OBA contract, Article 3(1) DCD empowers them with contractual remedies.[1277]

Therefore, Article 3(1) DCD brings OBA contracts for digital services within the scope of the Consumer Rights Directive (CRD) and Unfair Contract Terms Directive (UCTD). This suggests that digital service providers have to ensure the validity of consent under Article 7 GDPR and consumer protection rules regarding information disclosure, formation of contracts, withdrawal, non-conformity, remedies, and provision of gratuitous content.[1278] In other words, the validity of consent has to satisfy further contractual rules on incapacity, mistake, fraudulent behavior, or exploiting vulnerability through coercion or manipulation.[1279] Therefore, in case consent to OBA is found to be invalid, digital service providers would not only breach the GDPR but also national contract rules that entitle consumers to remedies such as damages.[1280] Consumer protection law helps consumers demand the provision of services agreed upon via OBA contracts.[1281]

One of the central requirements of CRD is informing consumers about the total price of a contract.[1282] However, digital service providers are exempt from the requirement to disclose the exact "price" of OBA contracts.[1283] This exclusion is likely put in place to avoid putting a "price" on personal data. Nevertheless, without disclosure of costs, OBA contracts seem to have less protection than contracts with a monetary fee, that also seems counterintuitive. To remedy this asymmetry, some have suggested that disclosing the monetary value that digital service providers earn via OBA contracts can provide "material information" to consumers when agreeing to such an exchange.[1284] Information about the costs can also entail appropriate disclosure of risks regarding entering OBA contracts.

In case personal data is regarded as a direct counter-performance to OBA contracts, an interesting implication may be that such contractual counter-performance may be taxed.[1285] Yet, it is unlikely that any state will give such an

[1277] *See Id.*

[1278] Marco Loos et al., *The Regulation of Digital Content Contracts in the Optional Instrument of Contract Law*, 6 EUR. REV. PRIV. L. 729, 733 (2011).

[1279] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 98.

[1280] *See* Helberger, Zuiderveen Borgesius & Reyna, *supra* note 41, at 10.

[1281] *See Id.*, at 2.

[1282] *See Id.*, at 10.

[1283] Digital Content Directive, *supra* note 940, art. 2(7). *See* Helberger, Zuiderveen Borgesius, & Reyna, *supra* note 421, at 13.

[1284] *See e.g.,* Malgieri and Custers, *supra* note 1273. *See also* Sarah Spiekermann & Jana Korunovska, *Towards a Value Theory for Personal Data*, 32 J. INF. TECHNOL. 62 (2017).

[1285] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 77.

interpretation, especially considering the re-assertion in the DCD that personal data is not a commodity.[1286]

6.3.2. Contractual Necessity

Generally, consent is not the only legal basis for digital service providers to process consumer data. Article 6(1)(b) GDPR allows the processing of personal data when this is "necessary for the performance of a contract".[1287] This provision considers that sometimes contracts cannot be performed, and services cannot be provided if the consumer does not provide personal data.[1288] This is when a consumer pays with a credit card for a product available on an online marketplace and requests its delivery to their home address.[1289] In this case, Article (6)(1)(b) GDPR allows the online marketplace to process the consumer's card details and address based on this clause.[1290]

On May 25, 2018, when the GDPR came into force with strengthened requirements for consent, Meta updated its terms and conditions, stating that it processed the consumer personal data under Article 6(1)(b) GDPR because such data was necessary to perform "core service" of Meta's platforms (Facebook, Instagram), now framed as "personalized experience", including personalized advertisement.[1291] On the same day, *Noyb*, a digital rights organization that can be said to act as the "private prosecutor" for enforcing the GDPR,[1292] filed a complaint with the Austrian DPA.[1293] Noyb argued that Meta attempted to bypass the GDPR's strict consent requirements and engaged in illegitimate OBA.[1294] As Meta's EU head office is located in Ireland, the Austrian DPA transferred the case to the Irish DPA.[1295]

[1286] *See* Digital Content Directive, *supra* note 940, rec. 24.

[1287] General Data Protection Regulation, *supra* note 44 at art 6(1)(b).

[1288] EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, 2 (2019).

[1289] *Id.* at 35.

[1290] *Id.*

[1291] *See BREAKING: Meta Prohibited from Use of Personal Data for Advertising*, NOYB (2023), https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising (last visited May 2, 2023).

[1292] Noyb stands for "none-of-your-business". Full name of this organization is European Center for Digital Rights. *See* CPDPConferences, *supra* note 945.

[1293] *See* noyb, *Noyb.Eu Filed Complaints over "Forced Consent" against Google, Instagram, WhatsApp and Facebook*, NOYB (2023), https://noyb.eu/en/noybeu-filed-complaints-over-forced-consent-against-google-instagram-whatsapp-and-facebook (last visited May 2, 2023).

[1294] *See Id.*

[1295] *Decision of the Data Protection Commission made pursuant to Section 113 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, (Dec. 31, 2022) (Ir.),* 49.

In 2014, the EDPB already argued that contractual necessity was not a suitable legal ground for OBA within the context of the 1995 Data Protection Directive that preceded the GDPR.[1296] In 2019, the EDPB reiterated that digital service providers could not rely on Article 6(1)(b) GDPR as the legal basis for OBA.[1297] However, in 2021, the Irish DPA published a *draft* decision suggesting that Meta relied on valid legal grounds. The reasoning of Irish DPA supported the argument that *if* OBA was Meta's core service to consumers, then processing personal data for OBA was, indeed, necessary. Irish DPA avoided evaluating the validity of tha claim that OBA constituted Meta's sprimary service to consumers, pointing to the competence of the contract law, and outside of the competence of the DPA.

After several EU DPAs objected to the draft decision, the Irish DPA referred the case to the EDPB, which in July 2022 issued binding decisions that clarified that Meta when serving Facebook provided social networking service could not rely on the contractual necessity clause as the legal basis for processing personal data for OBA.[1298] The EDPB argued that OBA involves processing an open-ended amount of consumer personal data and cannot be "strictly necessary" for the contract, even if the subject of the contract is personalization (including personalized advertising).[1299] The EDPB explained that while it may be less profitable, Meta could personalize advertisements based on limited consumer data, such as what consumers disclose when they sign up (e.g., age, gender, and country of residence).[1300] The EDPB further states that accepting contractual necessity as a valid legal basis for OBA would make lawful "theoretically any collection and reuse of personal data".[1301]

In accordance with the EDPB's binding decision, on 31 December 2022, the Irish DPA issued a €390 million fine to Meta, banned the company for engaging in OBA on the basis of Article 6(1)(b) GDPR, and gave the company three months to bring their OBA practices in compliance to the GDPR.[1302] In response to this decision, Meta updated its terms and conditions, and since April 5, 2023, it has continued to process personal data for OBA based on their claimed "legitimate

[1296] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)*, 17 (2017). ("[Contractual necessity] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his clickstream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example.")

[1297] *See* EUROPEAN DATA PROTECTION BOARD, *supra* note 1288 at 51–56.

[1298] *See generally* Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, European Data Protection Board (Jul. 28, 2022).

[1299] Data Protection Commission (Ir.) (Dec. 31, 2022), *supra* note 1295, 49.

[1300] European Data Protection Board (Jul. 28, 2022), *supra* note 1297, 132.

[1301] *Id.*

[1302] Data Protection Commission (Ir.) (Dec. 31, 2022), *supra* note 1295, 113.

interest" under Article 6(1)(f) GDPR.[1303] Section 6.3.3 analyzes the validity of relying on legitimate interest for OBA.

6.3.3. Legitimate Interest

On 4 July 2023, the CJEU published its judgment in the *Meta v. Bundeskartellamt* case.[1304] Among other questions related to Meta's OBA practices, the CJEU considered whether Meta could rely on Article 6(1)(f) GDPR to process consumers' personal data for OBA. The court echoed the earlier guidance of the EDPB that the legitimate interest clause under Article 6(1)(f) GDPR requires that the processing of personal data meets three cumulative conditions:[1305] (i) the publishers have a legitimate purpose; (ii) processing of personal data is necessary to meet this purpose ("necessity test"); and (iii) this purpose is balanced against the consumers' interests and fundamental rights ("balancing test").[1306] The CJEU evaluated the case based on these criteria and established that Meta's reliance on Article 6(1)(f) GDPR for OBA was not compliant with the GDPR.[1307]

Regardless of the CJEU judgment in the *Meta v. Bundeskartellamt* case, Meta continued to process behavioral data on the ground of the "legitimate interest".[1308] On 14 July 2023, the Norwegian DPA introduced "urgent and provisional measures" against Meta, banning the company's OBA practices for three months within Norway.[1309] It also referred the issue to the EDPB, which on October 27, 2023 decided to extend the ban on Meta's OBA practices across the EU.[1310] The Norwegian DPA conducted a thorough analysis of Article 6 (1)(f) GDPR based on the three conditions (legitimate purpose, necessity, and balancing test), which can be

[1303] *See How Meta Uses Legal Bases for Processing Ads in the EU,* META, *supra* note 210.

[1304] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017.

[1305] *Id.* at 106.

[1306] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)*, (2014). *See* Zuiderveen Borgesius, *supra* note 1210 at 167–170.

[1307] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017, at 117. ("[I]n this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalized advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR.")

[1308] Norwegian Data Protection Authority (Datatilsynet) Urgent and Provisional Measures - Meta 21/03530-16 (Jul. 14, 2023) (No.), https://shorturl.at/akEIR (last visited Jul 20, 2023).

[1309] *Id.*

[1310] *See* European Data Protection Board Press Release. "EDPB Urgent Binding Decision on processing of personal data for behavioral advertising by Meta", 1 November 2023. https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en Norway is not a Member State of the EU, but is a member of European Economic Area. The GDPR applies to Norway, and NO DPA is a member of the EDPB.

extrapolated to apply to all digital service providers that would like to rely on Article 6(1)(f) for engaging in OBA.

Firstly, digital service providers must have a legitimate purpose – they cannot have a mere legitimate interest in engaging in prohibited practices. This means that digital service providers cannot claim a legitimate purpose to engage in forms of OBA that are explicitly prohibited (section 6.2). Assuming that some forms of OBA are not prohibited, engaging in such forms of OBA could potentially provide a valid, legitimate purpose.[1311] OBA is sometimes claimed to provide "relevant ads" and are thus preferable to consumers.[1312] The argument that OBA is in line with consumer preferences and that digital service providers can thus process personal data without asking consumers to share their preferences (by consent) is illogical and indefensible.[1313] There are three other ways such legitimate purpose is typically framed: (1) OBA is claimed to enable "free internet" and support digital media (e.g., online newspapers) by funding digital services without consumer paying a monetary fee;[1314] (2) OBA is also a form of marketing, which is a legitimate interest for any businesses, and (3) OBA also serves a purpose of maximizing the profit for publishers.[1315] All these aims can be considered legitimate given that they pass the necessity and balancing test of Article 6(1)(f) GDPR.

Secondly, arguably first two aims listed in the previous paragraph cannot pass the necessity or proportionality test of Article 6(1)(f) GDPR. This test implies that processing data is "strictly necessary" only for predetermined ends that cannot be attained by processing less data.[1316] OBA is not the only way digital service providers can engage in marketing or monetize consumer attention.[1317] Broad demographic (segmented) and contextual advertising provide alternative marketing strategies that can act as alternatives for funding the digital industry (section 6.3.1.1).[1318] In contrast, the third aim listed in the previous paragraph, maximizing publisher profit, seems likely to pass the necessity test.[1319]

[1311] CHEN, *supra* note 947 at 2.

[1312] Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308, 16 (2023). ("Meta's allegation that Behavioral Advertising is in line with data subject's preferences, appears leveraged as an argument for why data subjects should not be able to freely exercise their preferences, which seems rather illogical.")

[1313] *Id.*

[1314] CHEN, *supra* note 947 at 55. As Chen also concludes, other claims about OBA promoting innovation and supporting democracy is by giving access to the options over the internet seem far-fetched.

[1315] Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308, 17.

[1316] *See* European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, 63.

[1317] Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308 at 17.

[1318] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017, at 150. *See also* European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 119.

[1319] Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308 at 17.

Indeed, it is possible that publishers engage in advertising that is based on personal data explicitly disclosed by the consumers when they sign up for the service (e.g., name, age, gender).[1320] There is a perception in the industry that OBA generally optimizes return on invested capital in advertising.[1321] OBA, which involves processing almost unlimited amounts of data, can be more profitable than alternative models, at least for publishers with access to consumer data, such as Alphabet and Meta (section 2.3.3).[1322] In 2019, the UK Competition and Markets Authority (CMA) published a comprehensive study about the advertising practices of these two companies and found that their profits far exceeded fair estimates.[1323] The CMA attributes these excess profits to the control of data exercised by these gatekeepers, which gives them a competitive advantage in online advertising, implying the centrality of OBA in maximizing their profits.[1324]

Thirdly, publishers' aim to maximize profit via OBA can not satisfy the "balancing test" of Article 6(1)(f) GDPR.[1325] Indeed, the largest share of the online advertising industry can be attributed to OBA, with a yearly turnover of nearly €100 billion in Europe.[1326] Therefore, if OBA is argued to facilitate publishers to earn excess profits, such profit maximization can be considered a legitimate end pursued within the "freedom to do business". Still, this legitimate end has to be balanced against the consumer's interests. In light of the consumer interests identified in Chapter 5 of this thesis, profit maximization can never outweigh interests under threat due to OBA, including threats to their integrity and dignity that are considered *inviolable* in the EU.[1327]

[1320] Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017, at 150. *See also* European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 119.

[1321] This perception in the industry is not necessarily grounded in the empirical evidence. *See* European Commission Study Recent Digital Advertising Developments, *supra* note 36 at 115.

[1322] Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308 at 17.

[1323] CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 67. ("We have found through our profitability analysis that the global return on capital employed for both Google and Facebook has been well above any reasonable benchmarks for many years. We estimated that the cost of capital for both Google and Facebook in 2018 was around 9%, whereas their actual returns have been substantially higher, at least 40% for Google's business and 50% for Facebook. This evidence is consistent with the exploitation of market power.")

[1324] *Id.*, at 15. ("Advertisers and media agencies have told us that Google offers in-depth targeting options, driven by its unique and vast sources of data, while Facebook has the advantage of offering the ability to target specific audiences based on demographic characteristics, interests and location. This creates a substantial competitive advantage for Google and Facebook, both of which have access to more extensive datasets than their rivals.")

[1325] *See* Zuiderveen Borgesius, *supra* note 1210 at 167–170.

[1326] In 2016, 86% of digital advertising revenue in Europe was estimated to be derived from using behavioral data, with the predictions that such reliance would increase over time. The Value of Digital Advertising, *supra* note 174. *See also Digital Advertising - Europe*, STATISTA, https://www.statista.com/outlook/dmo/digital-advertising/europe (last visited May 2, 2023).

[1327] *See* Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308 at 18-20.

The CJEU and Norwegian DPA decided that Article 6(1)(f) GDPR was not a legitimate basis for Meta to engage in OBA, given that Meta, which is considered a gatekeeper in the EU, has significant market power.[1328] The DMA further clarifies that designated gatekeepers must rely on consumer consent when processing data for OBA using data collected by third parties.[1329] The Belgian DPA's decision concerning the IAB Europe's TCF also suggests that publishers cannot rely on Article 6(1)(f) GDPR for OBA, at least within the AdTech ecosystem in which numerous parties are involved.[1330] In case the industry evolves, there may be some room for small publishers (e.g., newspapers, blogs) to use such a legal basis in limited cases. However, in the industry's current state, consumer consent is the only legitimate legal ground for engaging in OBA, including sharing data with third parties.

6.4. OBA Transparency & Fairness

The EU legal framework sets boundaries for consumer manipulation via OBA by explicitly prohibiting certain OBA practices and allows OBA only if it meets legal requirements of Article 6(1)(a) GDPR by acquiring consumers' valid consent. The EU legal framework sets further boundaries for consumer manipulation via OBA by laying down rules on transparency and fairness when engaging in OBA. Section 6.3.1. elaborates on information disclosure requirements for digital service providers that show online advertisements. Section 6.3.2. explains how DSA's additional online advertising transparency requirement for VLOPs/VLOSEs can limit consumer manipulation via OBA. Section 6.3.3. elaborates on risk assessment and mitigation measures required for various digital service providers in the EU legal framework and their role in setting boundaries to consumer manipulation via OBA.

6.4.1. Information Disclosure

Article 26 (1) DSA requires "online platform" providers that show ads on their interface to disclose certain information.[1331] Article 26 (1) (a) DSA requires disclosure that the "information is an advertisement".[1332] Identification of online advertisements as such is suggested to include standardized visual or audio marks.[1333] The DSA suggests that for such identification, "online platforms" can

[1328] *Meta v.* Bundeskartellamt [BKartA] Case VI-Kart 1/19 (V), Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (Facebook), 26 August 2019, ECLI:DE:OLGD:2019:0826.VIKART1.19V.0A (Ger.), *supra* note 1015.

[1329] Digital Markets Act, *supra* note 14, art. 5(2).

[1330] *See* Veale and Zuiderveen Borgesius, *supra* note 31, at 20.

[1331] Digital Services Act, *supra* note 2, art. 26(1).

[1332] *Id.,* art. 26(1)(a).

[1333] *Id.,* art. 26(1)(a), art. 44(h).

follow the standards set by "relevant European and international standardization bodies." [1334] Article 26(1)(b) DSA requires "online platforms" to disclose "a natural or legal person on whose behalf advertisement is presented."[1335] This is likely to mean that the name of the advertiser has to be identified. Article 26(1)(c) DSA requires identification of "a natural or legal person who paid for the advertisement" if this person is different from the advertiser.[1336]

There is some ambiguity regarding the disclosure requirement of Article 26 (1)(c) DSA. Advertisers can be serviced by various intermediaries, such as ad networks, media agencies, Demand Side Platforms (DSPs), and advertiser ad servers (section 2.3.2). At times, ad networks (e.g., Google Display Network) may provide complete intermediation, including pay "online platform" to place an ad, and in this case, it seems likely that Article 26(1)(c) DSA would require disclosure of an ad network as a payer. In cases where advertisers are served by multiple intermediaries, it seems that Article 26(1)(c) DSA would only cover a payer (e.g., media agency) and leave out other beneficiaries (e.g., DSP) that benefit from ad placement.

Article 26(1)(d) DSA also requires "online platform" providers to disclose "meaningful information" about the "main parameters used to determine" who receives the advertisement.[1337] Recital 68 DSA clarifies that disclosure has to provide "meaningful explanations of the logic used […], including when this is based on profiling."[1338] Such disclosure has to "include information on the method used for presenting the advertisement."[1339] In the context of OBA, these clarifications suggest that consumers of "online platforms" must be able to identify when an advertisement is personalized based on consumer behavior (i.e., "profiling"). However, identifying the criteria the OBA algorithm relies on to target consumers may be more challenging. What criteria can be considered meaningful under Article 26(1)(d) DSA can be interpreted differently. Note that Article 26 (1)(d) DSA requires "online platforms" to allow consumers to change targeting criteria, "where applicable."[1340]

The narrowest interpretation would consider it enough to include broad demographic or contextual information about location, language, age, and gender and the disclosure that it relies on behavioral personalization (profiling).[1341] However, it is unlikely such a disclosure would be "meaningful" under Article

[1334] *Id.*, art. 44.
[1335] *Id.,* art. 26(1)(b).
[1336] *Id.,* art. 26(1)(c).
[1337] *Id.,* art. 26(1)(d).
[1338] *Id.,* art. 68.
[1339] *Id.*
[1340] *Id.,* art. 26(1)(d).
[1341] e.g., disclosure of profiling can be as limited as: *"To predict which ads you might like, we also consider your ad preferences, activity and other factors."* It is doubtful that such note can amount to "meaningful" disclosure.

26(1)(d) DSA. Instead, broader interpretation would require disclosure of the criteria with which consumer was profiled, and type of data used for profiling. On February 14, 2023, Meta introduced a new advertising transparency tool on Facebook that allows disclosure of the criteria that their OBA algorithm relies on.[1342] Whether such information disclosure provides sufficient transparency to safeguard against consumer manipulation via OBA depends on how strictly the DSA is enforced. Without adequate enforcement, there is a risk that such disclosures increase consumers' perception of online advertising trustworthiness but still maintain certain essential aspects of targeting hidden from the consumer (section 4.3.1.).

Exceptionally opaque OBA practices are "lookalike" and "custom" audiences, in which targeting happens algorithmically, and derived criteria can reveal information of limited relevance (e.g., cursor movement similar to other consumers). In addition to the DSA rules, using such algorithmic systems will require digital service providers to comply with AIA—Article 52 EC.AIA can be understood to require digital service providers to disclose that consumers are interacting with an AI system.[1343] Article 52 EC.AIA will apply to all digital service providers using AI systems, in contrast to Article 26(1) DSA that only applies to " online platforms".

In addition, the DSA also includes information disclosure rules for recommender systems. Such recommender systems can influence consumers to extract their attention, time, and data and, thus, contribute to consumer manipulation via OBA (section 2.2.2).[1344] The harms to integrity and dignity by such systems are particularly notorious.[1345] Therefore, Article 27 DSA requires "online platforms" to disclose the main parameters used for personalization and how the consumers can influence these parameters.[1346]

In contrast to Article 26 DSA requirements regarding advertising, recommender system information can be disclosed in the terms and conditions. Article 27 (3) DSA requires "online platforms" to offer functionality by which consumers are able to select and modify their preferred options for recommendations.[1347] Article 38 DSA also clarifies that VLOPs/VLOSEs are required to provide at least one alternative that is not based on behavioral personalization ("profiling").[1348]

[1342] *See* Increasing Our Ads Transparency, META (Feb. 14, 2023), https://about.fb.com/news/2023/02/increasing-our-ads-transparency/ (last visited Oct 23, 2023).

[1343] AI Act Proposal, *supra* note 53, art. 52.

[1344] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 59.

[1345] *Id.*

[1346] *See* Maarten Rijks & Annemijn Schipper, *The DSA: Advertising, Dark Patterns and Recommender Systems*, TALORWESSING (Dec. 15, 2022), https://www.taylorwessing.com/en/interface/2022/the-eus-digital-services-act/the-dsa-advertising-dark-patterns-and-recommender-systems (last visited May 11, 2023).

[1347] *Id.*

[1348] Digital Services Act, *supra* note 2, art. 39.

Lastly, while Article 26(1) DSA requirements do not apply to digital service providers other than "online platforms", it guides as to what information can be regarded as "meaningful" under Article 7 UCPD, omission of which can qualify OBA as misleading. The consumer protection authorities can rely on the UCPD to ensure all digital service providers that engage in OBA in a way that holds the potential to manipulate consumers (e.g., third-party advertising in AdTech) disclose information required by Article 26(1) DSA for online platforms, including targeting criteria. With this in mind, Article 44(h) DSA encourages the European Commission and the European Digital Service Board (EDSB) to support the development of online advertising standards.[1349] This thesis recommends that EDSB contributes to the EDPB to provide updated guidance on OBA that clarifies what can be considered meaningful information disclosure in the context of varying sizes of publishers, including for VLOPs/VLOSEs (section 7.2).

6.4.2. OBA Scrutiny: Archives, Access, Audit

Article 39 DSA requires the providers of VLOPs/VLOSEs (e.g., YouTube, Facebook, TikTok) that engage in OBA to publish advertising "repositories" or archives.[1350] In particular, VLOPs/VLOSEs are obliged to "compile and make publicly available in a specific section of their online interface through a searchable and reliable tool that allows multicriteria queries and through application programming interfaces [APIs] a repository containing the [following] information:" (a) the advertising content, (b) advertiser; (c) payer; (d) the advertising period; (e) if an advertisement was targeted and if so, targeting criteria; and (g) the number of consumers that the advertising reached and targeted.[1351]

The Article 39 DSA requirements are intended "to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation, and equality."[1352] In contrast to Article 26 DSA information disclosure requirements that are intended to ensure consumer transparency, Article 39 DSA provides transparency for the European Commission and other supervisory authorities, including the EBDS, the EDPB, national DPAs, consumer protection authorities (CPAs) and competition authorities (CAs). Apart from enforcers, Article 39 (3) DSA clarifies that advertising

[1349] *Id.,* art 44 (h).

[1350] Digital Services Act, *supra* note 2, art. 39.

[1351] *Id*. Article 39 (2)(f) does not relate to OBA, but the sponsored content that is relevant for example, in the context of influencer marketing.

[1352] Digital Services Act, *supra* note 2, rec. 95.

repositories also provide transparency for the public (e.g., media watchdogs)[1353] and "the relevant, vetted researchers" from academia.[1354]

Academia has long been concerned about the potential harms of OBA, practices of which have been challenging to scrutinize.[1355] In response to the Cambridge Analytica scandal, Alphabet[1356] and Meta[1357] have provided advertising repositories since 2018.[1358] These early forms of advertising repositories had a variety of shortcomings; for example, they were limited to political advertising and did not offer information regarding the targeting criteria used.[1359] In August 2023, Alphabet and Meta updated repositories to comply with Article 39 DSA, making all advertisements shown on their platforms available to the public.[1360] Neither of these repositories entails disclosing criteria for behavioral personalization (e.g., predicted interests), and it seems that Meta does not even disclose if behavioral personalization occurs.[1361]

Article 39 (2)(e) DSA requires VLOPS/VLOSEs to publish information about "whether the advertisement was intended to be presented specifically to one or more particular groups of recipients of the service and, if so, the main parameters used for that purpose including where applicable the main parameters used to exclude one or more of such particular groups." Recital 95 DSA clarifies that this information should include information about both targeting and delivery criteria.

The narrow interpretation of these provisions, which would consider VLOPs/VLOSEs not obligated to share meaningful information regarding behavioral personalization (profiling), decreases the potential value of such advertising repositories. Indeed, while malicious actors can use OBA practices to

---

[1353] *See generally* Paddy Leerssen et al., *News from the Ad Archive: How Journalists Use the Facebook Ad Library to Hold Online Advertising Accountable*, 26 INF. COMMUN. SOC. 1381 (2023). *See also* Supporting election integrity through greater advertising transparency, GOOGLE (2018), https://blog.google/outreach-initiatives/public-policy/supporting-election-integrity-through-greater-advertising-transparency/ (last visited Oct 23, 2023).

[1354] Digital Services Act, *supra* note 2, art. 39(3).

[1355] *See e.g.,* Calo, *supra* note 38. *See* Susser, Roessler & Nissenbaum, *supra* note at 12–29.

[1356] *See* Ads Transparency Center, GOOGLE ADS (2023), https://adstransparency.google.com/ (last visited Oct 21, 2023).

[1357] *See* Ad Library, META (2023), https://www.facebook.com/ads/library/ (last visited Oct 23, 2023).

[1358] *See generally* Leerssen et al., *supra* note 1353. *See also* Supporting election integrity through greater advertising transparency, *supra* note 1353.

[1359] *See* Leerssen et al., *supra* note 1353.

[1360] *See* New Features and Additional Transparency Measures as the Digital Services Act Comes Into Effect, META (Aug. 22, 2023), https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/ (last visited Oct 23, 2023).

[1361] *See* Ad Library, META (2023), https://www.facebook.com/ads/library/ (last visited Oct 23, 2023). *See* Ads Transparency Center, GOOGLE ADS (2023), https://adstransparency.google.com/ (last visited Oct 21, 2023). Note that these systems get updated often. This thesis addesses Alphabet and Meta repositories as they were in October 2023.

manipulate consumers or spread disinformation (such as in the Cambridge Analytica), the more systemic and inherent risk of OBA is that algorithmic targeting practices of platforms themselves can deliberately or negligently exploit consumer vulnerabilities (Chapter 4).[1362] Unless VLOPs/VLOSEs provide meaningful information regarding their behavior personalization practices, Article 39 DSA fails to provide the information needed to identify consumer manipulation via OBA.

Article 39 (3) DSA clarifies that advertising repositories provide transparency not only for the enforcers but also for "the relevant vetted researchers."[1363] Article 40 (8) DSA explains that the status of "vetted researcher" is granted by the Digital Services Coordinator (DSC) to the applying academic researchers with the "sole purpose of conducting research that contributes to the detection, identification, and understanding of systemic risks" in the EU.[1364] Further, Article 40 DSA provides enforcers and vetted researchers the power to request "access to or reporting of specific data, including data related to algorithms."[1365] Recital 96 DSA suggests that such requests can relate to recommender systems and advertising algorithms.[1366] Article 40 DSA requirements regarding access to data and algorithms provide a solid mechanism, but it largely depends on the extent to which the European Commission operationalizes it to enforce the boundaries of the EU legal framework in relation to consumer manipulation harms.

Article 15 DMA provides further scrutability of OBA for the European Commission, as it obliges gatekeepers to submit "an independently audited description of any techniques for profiling of consumers that the gatekeeper applies."[1367] Recital 72 DMA clarifies that Article 15 DMA transparency rules put "external pressure on gatekeepers not to make deep consumer profiling industry standards."[1368] The DMA intends to increase contestability for businesses that do not have similar data and safeguard consumers from harm.[1369] The audit reports of the "profiling" practices, including OBA and recommender systems (section 2.2.2), are also to be shared with the EDPB to facilitate enforcement of the data protection

[1362] *See* Hacker, *supra* note 54.

[1363] Digital Services Act, *supra* note 2, art. 39(3).

[1364] *Id.*, rec. 95. Note that for the most of VLOPs/VLOSEs except Booking, AliExpress (the Netherlands), the DSC country is Ireland. However, as the European Commission is primarily responsible for enforcing the DSA rules for VLOPs/VLOSEs, the Irish DSC is expected to take a backseat. *See* Here is why Digital Services Coordinators should establish strong research and data units, DSA OBSERVATORY, (Mar. 10, 2023), https://dsa-observatory.eu/2023/03/10/here-is-why-digital-services-coordinators-should-establish-strong-research-and-data-units/ (last visited Oct 23, 2023).

[1365] Digital Services Act, *supra* note 2, art. 4.

[1366] *Id.*, art. 4.

[1367] Digital Markets Act, *supra* note 14, art. 15.

[1368] *Id.,* rec. 72.

[1369] *Id.,* rec. 72.

rules.[1370] Article 15(3) DMA also obliges designated gatekeepers to make an overview of the report available publicly.[1371] The first round of audit reports is expected in March 2024. Article 37 of the DSA also includes a requirement for VLOPs/VLOSEs to conduct independent audits to assess their compliance with the DSA.[1372]

In sum, the DSA and the DMA contain requirements that increase transparency concerning advertising and "profiling" techniques, including rules regarding advertising archives (repositories), enforcers' access to data and algorithms, and audits of profiling practices. These requirements provide solid legal tools that enable enforcers and external investigators (e.g., academia, and media watchdogs) to identify manipulative practices of OBA empirically. Such empirical evidence can be crucial in enforcing boundaries of consumer autonomy against harm.

6.4.3. Managing OBA Risks

Article 34 (1) DSA requires VLOPs/VLOSEs to "diligently identify, analyze, and assess any systemic risks" that stem from the "design or functioning of their service[…], including algorithmic systems."[1373] Article 34 (1) (b) clarifies that such risk assessment should take into consideration the severity and probability of actual or foreseeable harms to fundamental rights, such as human dignity (Article 1 CFREU), privacy (Article 7 CFREU), personal data protection (Article 8 CFREU), freedom of expression (Article 11 CFREU), non-discrimination (Article 21 CFREU), children's rights, and consumer protection (Article 38 CFREU).[1374] Article 34 (2) DSAclarifies that such risk assessment is particularly relevant in the context of recommender and advertising systems.[1375] Recital 84 DSA clarifies that VLOPs/VLOSEs should focus on all relevant algorithmic systems, paying attention to data collection and use practices.[1376]

This thesis has illustrated that many OBA practices are highly likely to exploit consumer vulnerabilities (Chapter 4), and that this can lead to harms of varying severity, such as individual economic detriment or consumer humiliation by systemic threat of vulnerability exploitation (Chapter 5). Understood this way, Article 34 (1) DSA would require VLOPs/VLOSEs to include in their risk assessment evaluation how their OBA practices, including recommender systems, may result in consumer manipulation and consequent harm. Recital 81 DSA is explicit with regards to manipulating minors, requiring VLOPs/VLOSEs to asses

[1370] *Id.*, art. 15 (1).
[1371] *Id.*, art. 15 (3).
[1372] Digital Services Act, *supra* note 2, art. 37.
[1373] *Id.*, art. 34 (1).
[1374] *Id.*, art. 34 (1) (b).
[1375] *Id.*, art. 34 (2).
[1376] *Id.*, rec. 84.

risks of their practices "in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour."[1377]

Most importantly, Article 35 DSA requires VLOPs/VLOSEs to "put in place reasonable and effective mitigation measures, tailored to specific systemic risks identified" in their risk assessments.[1378] Such risk mitigation measures may include "adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide."[1379] It is also important to highlight that the DMA can be understood to address the structural market risks of gatekeepers concerning consumer manipulation via OBA.[1380]

To some extent, acquiring consumer consent in accordance with Article 7 of GDPR can be considered to mitigate *some*, but not all, risks of consumer manipulation via OBA.[1381] The act of consent is a juridical act that waives the human rights prohibition of processing personal data but also creates a contractual relationship.[1382] In order for such a waiver to be considered valid, informational asymmetry regarding the risks must be corrected. In other words, it can be argued that consumers are able to consent to waive *only* the risks they were aware of, and consent can mitigate OBA risks *only* to the extent of consumer awareness. Article 35 (1) (i) DSA includes in the list of risk mitigation measures "taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information."[1383]

Even then, some risks are unacceptable; therefore, consumer consent cannot justify these risks in two layers. Firstly, unacceptable risks can be understood as significantly harmful outcomes for individuals, including physical or psychological detriment (integrity harms *in* section 5.2.6).[1384] Secondly, such risks can be conceptualized as significantly harmful outcomes for society, including threats to future generations, democracy, and consumer humiliation (dignity harms in section 5.2.7).[1385] It is this logic that different versions of Article 5(1)(a)-(b) AIA are attempting to codify. All prohibitions discussed in section 6.2 set the boundaries for

[1377] *Id.*, rec. 81.
[1378] *Id.*, art. 35.
[1379] *Id.*, art. 35.
[1380] Digital Markets Act, *supra* note 14, rec. 14.
[1381] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 100.
[1382] *Id.* at 98.
[1383] *Id.*, art. 35(1)(i).
[1384] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 98.
[1385] *Id.*

unacceptable harms, including individual economic detriment to consumers (Article 5 UCPD) or structural market harms (Article 5 DMA, Article 102 TFEU).

With this in mind, the DSA rules on risk assessment and mitigation measures (Articles 34 and 35 DSA) seem to provide a solid tool to hold VLOPs/VLOSEs accountable in that they do not engage in practices that lead to unacceptable risks, and they take appropriate measures to manage other risks, such as regarding data confidentiality risks (i.e., data breach risks). So far, the OBA industry has focused on innovating to mitigate data confidentiality harms. For example, Alphabet Privacy Enhancing Technologies (PETs) that are likely to replace advertising depending on third-party cookies allow the processing of large datasets necessary for behavioral personalization without ever disclosing personal data (section 2.4.3).[1386] While such measures mitigate the risks related to privacy harms (section 5.2.4), they do not tackle other consumer manipulation harms such as economic, environmental, affinity, authenticity, integrity, and dignity harms.

It is worth noting that while Article 34(1)(b) DSA does not mention evaluating risks to Article 37 regarding environmental protection, it requires such evaluation nevertheless.[1387] Recital 81 DSA clarifies that the risk assessment is not limited to fundamental rights listed in Article 34(1)(b) DSA.[1388] Therefore, it is appropriate for VLOPs/VLOSEs to conduct environmental protection risk evaluation regarding their OBA practices when there is a higher likelihood of consumer manipulation. The EC.AIA explicitly intends to safeguard against environmental risks of deployment and usage of AI systems.[1389] Moreover, AIA will likely provide additional risk assessment and mitigation measures concerning OBA more broadly. In particular, Article 40b EP.AIA classifies recommender systems as "online platforms," defined by the DSA as high-risk AI systems requiring conformity assessment and consumer-facing transparency.[1390] Article 40b EP.AIA rules provide additional protection to Article 27 DSA regarding recommender system transparency (section 6.4.1).

Lastly, the DSA risk assessment and mitigation measures discussed in this section are addressed to VLOPs/VLOSEs (e.g., YouTube, Facebook, Google Search). Indeed, when it comes to the risk of OBA, in particular, consumer manipulation via OBA, they primarily stem from the OBA practices of the providers of these platforms, in particular, Alphabet and Meta. Nevertheless, this does not mean that smaller digital service providers, such as other "online platforms" or publishers (e.g., online newspapers), are free from responsibility when they engage

[1386] *See How we achieve privacy through innovation*, GOOGLE (2023), https://blog.google/technology/safety-security/how-we-achieve-privacy-through-innovation/ (last visited Jun 6, 2023).

[1387] Digital Services Act, *supra* note 2, art. 34 (1).

[1388] *Id.*, rec. 81.

[1389] AI Act Mandates, *supra* note 367, at par. 13 [rec. (3)].

[1390] *Id.*

in OBA. OBA involves personal data processing, and Article 24 GDPR requires all digital service providers that use personal data for OBA to consider risks in their processing activities.[1391] Article 24 of the GDPR assigns the responsibility and burden of proof for complying with the GDPR to digital service providers.[1392] The principle of *fairness* requires digital service providers to balance their interests with consumer interests, to correct power asymmetries, and to ensure that digital service providers do not infringe on inviolable consumer interests of integrity and dignity, regardless of whether the consumer has consented to process data for OBA or not.[1393]

Article 35 GDPR operationalizes the fairness principle by requiring conducting a Data Protection Impact Assessment (DPIA) in high-risk situations.[1394] A29WP guidelines regarding DPIA adopted in 2017 do not explicitly require digital service providers to conduct DPIA in all cases in which they conduct OBA.[1395] Instead, as Article 35(3)(a) GDPR also clarifies in the example, OBA will require a DPIA in case it can be considered automated decision-making that has legal or similarly significant effects under Article 22 GDPR (section 6.2.3). Indeed, if OBA is limited to smaller-scale digital service providers and does not combine data from other sources, such OBA may be considered to have a low likelihood of algorithmic manipulation nor cause severe consumer manipulation harms. Nevertheless, making use of AdTech can have risks similar to OBA practices of VLOPs/VLOSEs. With this in mind, it is recommended that all publishers engaging in OBA via AdTech also conduct DPIA to evaluate and mitigate risks of consumer manipulation. In essence, failing to conduct such a risk assessment can also be considered a breach of Article 5 UCPD requirement of professional diligence.[1396]

In sum, the requirements regarding risk assessment and mitigation in the EU legal framework provide solid safeguards against consumer manipulation harms of OBA. These requirements deem digital service providers – gatekeepers even more so – as responsible for ensuring that their OBA practices do not lead to severe individual (integrity) or societal (dignity) harm. This section argues that consumer consent cannot justify exposing consumers to unacceptable risks.[1397] Therefore,

[1391] General Data Protection Regulation, *supra* note 44, recs. 42, 32, 58.

[1392] *Id.*

[1393] *See generally* Damian Clifford & Jef Ausloos, *Data Protection and the Role of Fairness*, 37 YEARB. EUR. L. 130 (2018).

[1394] General Data Protection Regulation, *supra* note 44, at 5(1)(a), art. 35.

[1395] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, Wp248rev.01*, (2017), https://ec.europa.eu/newsroom/article29/items/611236/en (last visited Oct 24, 2023).

[1396] *See* Hacker, *supra* note 54.

[1397] This argument is grounded in the logic of the CJEU judgment in *Omega* case C-36/02 Omega Spielhallen, 2004 E.C.R. 614., *supra* note 866. Moreover, famous "Dwarf Tossing" case from

OBA is legitimate only in case the consumer has expressed a genuine wish for behaviorally personalized advertisement, when such personalization is transparent (including regarding targeting criteria), and when digital service providers ensure that they have adequate measures to safeguard against systematic exploitation of vulnerabilities and societal harms.

6.5. Conclusion: Boundaries of Consumer Manipulation via OBA

This section answers SQ5 of this thesis:

SQ5: what are the boundaries of consumer manipulation via OBA in the EU?

The EU legal framework imposes legal boundaries on OBA mainly through three areas of law: consumer protection law, data protection and privacy law, and competition law. Other pieces of legislation within the remit of the EU digital single market provide essential parts for setting boundaries to consumer manipulation via OBA. Table 6-2 below summarizes the legal instruments within the EU legal framework discussed in the chapter.

Table 6-2. The EU Legal framework for consumer manipulation via OBA

EU Legal Framework	Section	Prohibition	Transparency *for* Consumer	Risk Mitigation	Transparency *for* Enforcer
EU Consumer Protection Law					
Unfair Commercial Practices Directive (UCDP)	6.1.1	X	X	X	
Consumer Rights Directive (CRD)			X		
Unfair Contract Terms Directive (UCTD)		X			
EU Personal Data Protection and Privacy Law					
General Data Protection Regulation (GDPR)	6.1.2	X	X	X	X
ePrivacy Directive		X	X		
EU Competition Law					
Treaty on the Functioning of the EU (TFEU)	6.1.3	X			
EU Digital Single Market Vision					
Audiovisual Media Services Directive (AVMSD)	6.1.4.1	X	X		
Digital Content Directive (DCD)					
Platform-to-Business Regulation (P2BR)					
Digital Services Act (DSA)	6.1.4.2	X	X	X	X
Digital Markets Act (DMA)		X	X	X	X
Proposal for Artificial Intelligence Act (ECAIA)	*6.1.4.3*	X	X	X	X
European Parliament Mandate (EP.AIA)		X	X	X	X
Council of the EU Mandate (CAIA)		X	X	X	X

France further illustrates this paradigm of putting forward public values (public morality) above individual autonomy and consent. *See* Susan Millns, *Dwarf-Throwing and Human Dignity: A French Perspective*, 18 J. SOC. WELF. FAM. L. 375 (1996).

This EU legal framework sets legal boundaries to consumer manipulation via OBA in four significant ways, putting in place: (i) prohibitions for unacceptable OBA practices; (ii) information disclosure rules and ensuring transparency for consumers; (iii) risk assessment and mitigation rules, thus ensuring fairness, and (iv) transparency and data access rules that enable enforcers to hold digital service providers accountable in their OBA practices (Table 6-2).

Firstly, Article 26 (3) DSA prohibits "online platforms" from using special categories of data for OBA (section 6.2.1).[1398] As children are considered particularly vulnerable, Article 28 (2) DSA prohibits "online platforms" from targeting minors using OBA.[1399] Article 6a (2) AVMSD includes the same prohibition for audiovisual service providers.[1400] Article 28 (2) DSA and Article 6a(2) AVMSD re-iterate the already existing consensus between data protection authorities (DPAs) that Article 8 GDPR entails a prohibition for all digital service providers to target minors with OBA (section 6.2.2).[1401]

Article 6 (1) GDPR prohibits all OBA unless an adult consumer gives digital service providers valid consent that adequately reveals their valid preferences (section 6.3).[1402] In *Meta v. Bundeskartellamt,* the CJEU found that significant market power can contribute to exploiting consumer vulnerabilities in consumer decisions for consenting to OBA and can also be regarded as an abuse of dominance under Article 102 TFEU (section 6.1.3).[1403] Article 5 UCPD provides a general prohibition of unfair commercial practices that can capture consumer manipulation via OBA entirely (section 6.2.4).[1404] If adopted, Article 5(1)(a)-(b) AIA provides additional prohibitions of consumer manipulation via OBA when it relies on AI systems (section 6.2.5).[1405]

[1398] Digital Services Act, *supra* note 2, art 26 (3) rec. 69. Recital 69 DSA suggests that Article 26 (3) DSA intends to safeguard consumers against manipulation via OBA. Nevertheless, due to the focus on categories of data instead of the problem at hand (consumer manipulation), it may be challenging to enforce Article 26 (3) DSA to capture all manipulative practices of OBA.

[1399] *Id.*, art 28 (3).

[1400] Audiovisual Media Services Directive, *supra* note 1026 art. 6a(2).

[1401] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 1128.

[1402] *See generally* Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1310. In addition, Article 22 GDPR requires higher standard (explicit) consent if OBA can have significant effects, such as when advertising employment opportunities or housing (section 6.2.3). General Data Protection Regulation, *supra* note 44, art. 6(1), 22.

[1403] *See* Case C-252/21, Meta v. Bundeskartellamt, ECLI:EU:C:2023:537, *supra* note 1017. In addition, in case OBA is offered by the designated gatekeepers (e.g., Alphabet and Meta), Article 5 DMA prohibits combining consumer data between their platforms (e.g., Facebook, Instagram) or from third parties without consumer consent. Recitals 36 and 37 DMA also prompt gatekeepers to offer a less personalized alternative to ensure consumer consent to OBA is freely given. *See* Digital Markets Act, *supra* note 14, art. 5, rec. 36, 37.

[1404] Unfair Commercial Practices Directive, *supra* note 42, art. 5.

[1405] AI Act Mandates, *supra* note 367 at par. 181-183.

Secondly, the EU legal framework requires digital service providers to make their OBA practices transparent for the consumers (section 6.4.1). Article 26(1) DSA requires "online platforms" to disclose information regarding OBA, such as the identity of an advertiser, ad intermediary, and ad targeting criteria.[1406] Article 7 UCPD can also be interpreted to require information for other digital service providers engaging in OBA.

Thirdly, the DSA, the DMA, the GDPR, the UCPD, and the AIA include rules that oblige various digital service providers to conduct risk assessments and adopt risk mitigation measures in order to ensure fairness. These rules impose responsibility on digital service providers that their OBA practices do not cause unacceptable (e.g., integrity and dignity) harms, and they mitigate harms to other interests (e.g., privacy) by technical or procedural measures (e.g., browser-based targeting).

Fourthly, the DSA and the DMA provide transparency and access rules that enable enforcers and public watchdogs to hold the most prominent platform providers (e.g., Alphabet, Meta) accountable, including in their OBA practices. While the UCPD captures the prohibition of all manipulative practices of OBA, classifying these practices to be unfair requires *ex-post* analysis. Also, consumer manipulation is most likely to stay hidden from the consumer, thus making it difficult to operationalize UCPD – a complaint-based tool. With this in mind, the EU transparency and data access rules for enforcers can facilitate operationalizing the UCPD.

In sum, consumer manipulation via OBA can be considered unacceptable in the EU. Operationalizing the EU legal framework to enforce the boundaries and safeguard against consumer manipulation harms is mainly dependent on effective enforcement. The enforcement action has been limited until the 2020s. Since then, enforcement of the GPDR, consumer protection, and competition law have picked up pace. In addition, since March 2024 European Commission will be able to effectively enforce the DSA and the DMA and safeguard the boundaries of the EU legal framework.

[1406] Digital Services Act, *supra* note 2, art 26(1).