



Universiteit  
Leiden  
The Netherlands

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

Zardiashvili, A.

### **Citation**

Zardiashvili, A. (2024, May 7). *Power and dignity: the ends of online behavioral advertising in the European Union*. Retrieved from <https://hdl.handle.net/1887/3753619>

Version: Publisher's Version  
License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)  
Downloaded from: <https://hdl.handle.net/1887/3753619>

**Note:** To cite this publication please use the final published version (if applicable).

## CHAPTER 7. CONCLUSIONS: THE ENDS OF OBA

This final chapter of this thesis is divided into three parts: Section 7.1 answers the central research question of this thesis, section 7.1 offers two recommendations regarding enforcement and guidance, and section 7.3 looks ahead to anticipate the central challenges for policymakers and scholars.

### 7.1. Conclusion

This section answers the central research question (RQ) of the thesis and substantiates the answer:

**RQ: to what extent can the European Union (EU) legal framework safeguard against the harms of consumer manipulation via online behavioral advertising (OBA)?**

The short answer to the RQ is that *the EU legal framework can safeguard against all harms stemming from consumer manipulation via OBA*. Forms of OBA that result in consumer manipulation can be regarded illegitimate within the EU legal framework: OBA can be legitimized only when consumers genuinely prefer to be targeted via this method and when digital service providers have appropriate safeguards in place to ensure that their OBA practices do not lead to consumer manipulation harms that consumer consent cannot legitimize (e.g., integrity, dignity, environment, market).

Online behavioral advertising (OBA) is an online phenomenon that shows consumers personalized advertisements based on their behavioral data.<sup>1407</sup> OBA is one of several configurations of online advertising – it entails targeting an individual consumer sorted into segments based on interests (“surf enthusiast”) or detailed demographic traits (“household income top 10%”) that artificial intelligence (AI) systems infer based on data about the consumer that digital service providers observe and monitor (in contrast to data that consumers voluntarily provide).<sup>1408</sup> The consumer data the algorithm relies on for inferring consumer interests may include, among others, web browsing or social media behavior, mouse cursor movements, geo-location, or keyboard strokes.<sup>1409</sup>

Large digital platform providers, in particular Alphabet and Meta, are the most prominent OBA publishers, allowing advertisers to advertise on websites and apps not only on their platforms (e.g., YouTube, Instagram) but also on other digital service providers (e.g., online newspaper publishers) that join their networks (e.g.,

<sup>1407</sup> See Boerman, Kruijkemeier, and Zuiderveen Borgesius, *supra* note 81, at 364.

<sup>1408</sup> See Zard and Sears, *supra* note 1, at 800.

<sup>1409</sup> See ZUIDERVEEN BORGESIOUS, *supra* note 25, at 35–38.

Google Display Network, Meta Audience Network).<sup>1410</sup> These advertising networks are closed ecosystems where platform providers have end-to-end control of OBA sales and are called “walled gardens”.<sup>1411</sup> Alphabet dominates the search advertising market, and Meta dominates the social media advertising market.<sup>1412</sup> In addition, Alphabet dominates the open exchange market for OBA, also called AdTech, where all advertising, intermediaries, publishers, and advertisers trade an ad space.<sup>1413</sup>

Executing OBA requires complex infrastructures. It includes AI systems that allocate advertising to consumers based on consumer behavioral data.<sup>1414</sup> Facilitating these AI systems requires tracing consumers over the Internet, which is typically done by placing so-called “cookies” on consumer devices. Digital service providers compete with each other either in walled gardens or on the AdTech open exchange, typically via real-time bidding (RTB) programmatic auctions.<sup>1415</sup> The RTB auction is typically won by the party with the most data about the consumer, resulting in competition for extracting consumer data. As large platform providers such as Alphabet and Meta control access to consumer data, they dominate relative OBA markets. The OBA industry is increasingly moving from third-party tracking to “local” or browser-based advertising methods that can further centralize power in online advertising within these platform providers.

This thesis refers to *consumer manipulation via OBA* as instances when digital service providers manipulate consumers to facilitate OBA (manipulative extraction) and use OBA in a way that leads to consumer manipulation (manipulative advertising personalization). Manipulation can be defined as a successful and intentional attempt of an agent to influence a target toward an outcome (determined by an agent) where an essential aspect of the influence remains hidden from the target, and the agent is aware that the method of influence is likely to exploit the target’s decision-making vulnerability.<sup>1416</sup> The persuasion knowledge model (PKM) provides one understanding of what essential aspects can be hidden (e.g., advertiser, advertising criteria, etc.). Therefore, consumer manipulation via OBA refers to the situation where digital service providers hiddenly influence consumers to give away their attention, time, and data or to act on a particular advertisement by targeting them with an influence that can exploit their decision-making vulnerabilities. Digital

---

<sup>1410</sup> See CMA (UK) Study Online Platforms & Digital Advertising Appendix M, *supra* note 182.

<sup>1411</sup> See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 19.

<sup>1412</sup> See CMA (UK) Study Online Platforms & Digital Advertising Appendix M, *supra* note 182

<sup>1413</sup> European Commission Press Release IP/23/3207, The Commission, *supra* note 47

<sup>1414</sup> European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 25.

<sup>1415</sup> See Veale and Zuiderveen Borgesius, *supra* note 31.

<sup>1416</sup> This account of manipulation is a synthesis of two different accounts. The first account is of manipulation as “hidden influence” by Susser, Roessler, and Nisseunbaum. See Susser, Roessler, and Nissenbaum, *supra* note 38. Second account is of manipulation as “careless influence” by Klenk. See Klenk, *supra* note 305 at 13.

---

---

service providers can be said to exert a manipulative influence if they deliberately target to exploit consumer vulnerabilities and also if they disregard that their OBA practices, including any design features of their online environment or any AI system that they deploy, are likely to exploit consumer decision-making vulnerability.

Consumer manipulation via OBA refers to situations when, for example, digital service providers design online interfaces with default features that maximize the data extraction from the consumer, such as auto-play, content personalization, endless feed, and gamification, at times, without alternatives, and transparency around the economic logic.<sup>1417</sup> The most prevalent manipulative practices of OBA are strategies that digital service providers use to acquire *consent* from consumers to give away their personal data: as the EU law permits OBA only in case consumers consent (section 6.3), digital service providers use a variety of manipulative (and coercive) patterns to influence consumers towards consenting.<sup>1418</sup> This form of consumer manipulation is particularly prevalent and easy to recognize.

On the other hand, consumer manipulation via OBA also occurs through advertising personalization practices that influence consumers toward a particular action (e.g., visiting a website and purchasing a product) and are likely to exploit consumer decision-making vulnerabilities.<sup>1419</sup> OBA practices can mislead consumers by hiding essential information about an advertisement, such as the identity of an advertiser. Digital service providers can also manipulate consumers by directly targeting consumer vulnerabilities with ads (e.g., targeting recently divorced) or by disregarding the fact that algorithms deployed can target a consumer in a way that exploits their vulnerability (e.g., in the case of lookalike audiences).<sup>1420</sup>

Consumer manipulation via OBA may lead to a direct economic loss to the consumer or structural harm through market failures, such as reduced innovation, reduced quality of content and services, increased prices, reduced welfare, and reduced trust in the market.<sup>1421</sup> It can also contribute to *environmental harm* due to an increase in carbon emission, battery overuse, and electronic waste, as well as negatively affecting animal welfare.<sup>1422</sup> It can lead to *affinity harms* such as discrimination and oppression of specific (often marginalized) groups.<sup>1423</sup> Its

---

<sup>1417</sup> European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53.

<sup>1418</sup> See e.g., Leiser, *supra* note 466.

<sup>1419</sup> See Strycharz and Duivenvoorde, *supra* note 361 at 7.

<sup>1420</sup> See GALLI, *supra* note 41.

<sup>1421</sup> See Zarsky, *supra* note 38 at 172. See Calo, *supra* note 38 at 1025. See European Commission Study Recent Digital Advertising Developments, *supra* note 56 at 136.

<sup>1422</sup> See generally Hartmann et al., *supra* note 797. See generally Pärssinen et al., *supra* note 797.

<sup>1423</sup> Wachter, *supra* note 80.

*privacy harms* include emotional distress, disturbance, thwarted expectations, and anxiety.<sup>1424</sup>

Generally, manipulation can be understood as “time theft” that leads to *authenticity harms* such as loss of (time for) consortium, leisure, and earnings.<sup>1425</sup> Consumer manipulation via OBA can also result in *integrity harms* that include severe adverse effects on mental and physical health and fitness (e.g., self-harm, loss of life).<sup>1426</sup> Lastly, consumer manipulation via OBA may lead to *dignity harm*, which this thesis conceptualizes in three ways: firstly, consumer manipulation via OBA can harm the dignity of a child. Secondly, it can harm the dignity of individuals by threatening democratic processes in their society. Thirdly, it can harm the dignity of consumers as a group by entrenching consumer exploitation as a profitable market practice (section 5.2.7).

The EU legal framework for consumer manipulation via OBA includes three areas of law: (1) consumer protection law, in particular, the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD), and the Unfair Contract Terms Directive (UCTD); (2) data protection and privacy law, in particular, the General Data Protection Regulation (GDPR), and ePrivacy Directive; and (3) competition law grounded in Article 101-102 Treaty of the Functioning of the EU (TFEU). The EU legal framework also includes other legislation adopted within the EU vision for the digital single market, in particular, the AudioVisual Media Services Directive (AVMSD), the Platform-to-Business Regulation (P2BR), the Digital Content Directive (DCD), the Digital Services Act (DSA), the Digital Markets Act (DMA), and initiatives for the Artificial Intelligence Act (AIA).

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

In theory, the EU legal framework can safeguard all consumer manipulation harms of OBA (Table 7-1). The individual pieces of the EU legal framework can safeguard some harms directly (**dark green** in Table 7-1). For example, the primary aim of the UCPD is to safeguard the economic interests of consumers by ensuring that they can exercise authentic choice. These legislative tools can also indirectly safeguard some consumer manipulation harms, either for ensuring the protection of primarily aimed interests or as a consequence of protecting primary interests (**light**

<sup>1424</sup> See Citron and Solove, *supra* note 625 at 841.

<sup>1425</sup> See generally Sunstein, *supra* note 831.

<sup>1426</sup> See Franklin et al., *supra* note 39. Molly Russell inquest, *supra* note 39.

green in Table 7-1). For example, the UCPD may require safeguarding consumer privacy when this is essential for consumer’s economic interests. Also, by ensuring authentic choice, the UCPD can also safeguard against other harms (e.g., affinity, dignity) that can occur in conjunction with economic harms the UCPD protects against.<sup>1427</sup>

Table 7-1 below illustrates the extent to which the EU legal framework can safeguard against consumer manipulation harms of OBA.

Table 7-1. Safeguarding against consumer manipulation harms of OBA: Dark green denotes the (primary) harms that the law intends to protect, and light green the harms that the law indirectly applies to while addressing the primary harms, and the harms that the law addresses in case they occur in combination with primary harms. The yellow boxes relate to the legislation that has limited or no applicability to indicated harms.

Consumer Manipulation Harms		The EU Legal Framework for Consumer Manipulation via OBA											
		Consumer Protection Law			Data Prot. & Privacy Law		Com. Law	Digital Single Market					
		UCPD	CRD	UCTD	GDPR	ePD	TFEU	AVSMD	P2BR	DCD	DSA	DMA	AA
Economic	Personal	Dark Green	Dark Green	Dark Green	Light Green	Light Green	Light Green	Yellow	Light Green	Dark Green	Light Green	Light Green	Yellow
	Structural	Dark Green	Light Green	Light Green	Light Green	Light Green	Dark Green	Light Green	Dark Green	Light Green	Light Green	Dark Green	Yellow
Environmental		Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Light Green	Yellow	Yellow	Light Green	Yellow	Dark Green
Affinity		Light Green	Light Green	Light Green	Dark Green	Light Green	Light Green	Dark Green	Light Green	Light Green	Light Green	Light Green	Dark Green
Privacy		Light Green	Light Green	Light Green	Dark Green	Dark Green	Light Green	Light Green	Light Green	Light Green	Light Green	Light Green	Dark Green
Authenticity		Dark Green	Dark Green	Dark Green	Dark Green	Light Green	Dark Green	Light Green	Light Green	Dark Green	Dark Green	Dark Green	Dark Green
Integrity		Light Green	Light Green	Light Green	Dark Green	Light Green	Light Green	Dark Green	Light Green	Light Green	Dark Green	Light Green	Dark Green
Dignity	Children	Light Green	Yellow	Yellow	Dark Green	Yellow	Yellow	Yellow	Yellow	Yellow	Dark Green	Light Green	Dark Green
	Democracy	Light Green	Yellow	Yellow	Light Green	Light Green	Light Green	Dark Green	Yellow	Yellow	Dark Green	Light Green	Dark Green
	Vulnerability	Light Green	Yellow	Yellow	Light Green	Light Green	Light Green	Dark Green	Yellow	Yellow	Dark Green	Light Green	Dark Green

In sum, consumer manipulation via OBA *can* be considered illegitimate in the EU. However, this conclusion is drawn from a close analysis of various pieces of legislation that can be misinterpreted, especially by the industry for whom consumer manipulation via OBA is profitable. Indeed, manipulative practices of OBA have proliferated in the online environment. This contradiction can be explained by the difficulty for the enforcers to break the silos and evaluate practices across different pieces of legislation, as done within this thesis.

<sup>1427</sup> See Guidance on the Interpretation of the Unfair Commercial Practices Directive, *supra* note 1155 at 1.1.1.1.

Enforcement has largely been left to national data protection authorities (DPAs) with limited mandates, capacity, and scope of their activities. *Meta vs. Bundeskartellamt* case further illustrates a competition authority (CA) breaking the silos. However, this case has been an exceptional precedent. Enforcement has been challenging as the OBA industry is incentivized to misinterpret the EU framework and continue to engage in consumer manipulation via OBA, that is highly profitable.

Nevertheless, the DSA and the DMA seem to provide the European Commission with sufficient powers to ensure that consumers in the digital markets can exercise authentic choice and are protected against exploitation. It does so by giving the European Commission powers to investigate the large platform providers or gatekeepers, such as Alphabet and Meta, who provide OBA infrastructures and set standards in the industry. These companies have to comply with the DMA by March 7, 2024, after which it is upon the European Commission to monitor and investigate their compliance and use the DMA as leverage to end consumer manipulation via OBA.

### 7.2. Recommendations

Following the conclusion of this thesis, safeguarding against consumer manipulation harms of OBA is dependent on the enforcement of the EU legal framework. This section provides two recommendations: (R1) bolder enforcement that applies the rules (more) strictly and breaks the silos of different legal domains, and (R2) issuing more precise guidelines that can help enforcers consistently apply the EU legal framework across the EU and clarify the rules for the industry.

*R1*: It is recommended that the European Commission, in its competence to enforce the DSA and the DMA, investigates the OBA practices (particularly of key players like Alphabet and Meta) in order to evaluate the extent to which these companies safeguard consumers against consumer manipulation harms.

In 2022, more than 50% of online advertising revenue went to Alphabet (\$168.44 billion) and Meta (\$112.68 billion).<sup>1428</sup> These companies are considered to operate as a quasi-duopoly in OBA markets, mainly due to their “data power” or competitive advantage in holding consumer data (section 2.3.3). Market studies increasingly find that OBA benefits these companies (other publishers and advertisers less so) at the expense of consumers.<sup>1429</sup> These companies are not only the standard-setters in the OBA industry but have also continuously demonstrated reluctance to comply with the EU legal framework in relation to their OBA practices.

---

<sup>1428</sup> See Shields, *supra* note 176.

<sup>1429</sup> See European Commission Study Recent Digital Advertising Developments, *supra* note 36 at 102.

Two of the most pressing cases for consumer manipulation via OBA are directly related to Alphabet and Meta. Firstly, the European Commission is considering forcing Alphabet to divest parts of its business due to its potential abuse of its dominant position in the AdTech market of OBA.<sup>1430</sup> Secondly, since the GDPR entered into force, Meta has engaged in a “catch-me-if-you-can” race against asking consumers for their consent for OBA under Article 6 (1) GDPR.<sup>1431</sup> The European Data Protection Board’s (EDPB) binding decision of October 27, 2023, suggests that Meta’s OBA practices have been illegitimate between 2018 and 2023.<sup>1432</sup> With this in mind, the OBA practices of these companies must be closely investigated, including compliance with Article 35 DSA measures regarding risk mitigation.

Article 56 (2) DSA gives the European Commission exclusive competence to enforce the DSA rules related to Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs), such as Alphabet and Meta.<sup>1433</sup> Article 51 DSA gives the European Commission power to investigate VLOPs/VLOSEs, including on-site inspections, and to request any information related to their compliance with the DSA.<sup>1434</sup> Further, Article 23 DMA gives the European Commission almost unlimited investigatory powers for gatekeepers such as Alphabet and Meta.<sup>1435</sup> Thierry Breton, the European Commissioner for the Internal Market has announced that the European Commission will concentrate its powers to enforce the DSA and the DMA rules.<sup>1436</sup>

The DSA and the DMA require Alphabet and Meta to submit risk assessments and audit reports, including with regard to their profiling practices. The European Commission will receive the latest auditing reports (for profiling techniques) in March 2024.<sup>1437</sup> Therefore, it is reasonable that the European Commission starts a formal investigation only after reviewing the first wave of reports provided by these companies. In order to adequately evaluate the OBA practices of the gatekeepers,

<sup>1430</sup> See European Commission Press Release IP/23/3207, The Commission, *supra* note 47

<sup>1431</sup> Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308.

<sup>1432</sup> See European Data Protection Board Press Release. “EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta”, 1 November 2023. [https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta\\_en](https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en) See also Datatilsynet, *Meta Case Brought to the European Level*, DATATILSYNET (2023), <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/meta-case-brought-to-the-european-level/> (last visited Oct 26, 2023).

<sup>1433</sup> Digital Services Act, *supra* note 2, 56 (2).

<sup>1434</sup> *Id.*, art. 51.

<sup>1435</sup> Digital Markets Act, *supra* note 14, art. 23.

<sup>1436</sup> See *Sneak peek: how the Commission will enforce the DSA & DMA*, EUROPEAN COMMISSION - EUROPEAN COMMISSION, [https://ec.europa.eu/commission/presscorner/detail/en/statement\\_22\\_4327](https://ec.europa.eu/commission/presscorner/detail/en/statement_22_4327) (last visited Oct 26, 2023).

<sup>1437</sup> Digital Markets Act, *supra* note 14, art. 15. Six months after a date of designation (September 6, 2023).



their potential for manipulation, and their harms, it is crucial that the European Commission adopts a holistic view of the EU legal framework and consults the EDPB, the European Digital Services Board (EDSB), the European Center for Algorithmic Transparency (ECAT),<sup>1438</sup> potentially European Artificial Intelligence Board (EAIB) and considers competition law, as well as consumer protection law implications of these practices.

Moreover, while gatekeepers are the standard-setters in the OBA industry, consumer experience in the online environment is mediated by millions of digital service providers that monetize their websites and apps via OBA. With this in mind, the boundaries of the EU legal framework must be enforced across the entire industry. This would require coordinated enforcement by national DPAs. In order to ensure that DPAs enforce the boundaries constantly across the EU, it is recommended that the EDPB provides further guidelines concerning OBA.

R2: It is recommended that the EDPB, within the scope of their mandate to clarify and promote a common understanding of the law, issues further guidelines on OBA.

While this thesis concludes that the EU legal framework can sufficiently safeguard against consumer manipulation harms of OBA, the boundaries of the legal framework are continuously challenged in practice, particularly elements that are unclear and have inconsistent enforcement. For example, national DPAs have reached conflicting decisions concerning the “OBA-or-Pay” model that the OBA industry is increasingly moving toward for monetizing digital services (section 6.3.1).<sup>1439</sup> Also, while the DSA and the DMA introduce OBA rules for VLOPs/VLOSEs and gatekeepers, there is ambiguity about the exact boundaries of these provisions. For example, Article 26(3) DSA prohibits engaging in OBA using special categories of data (Article 9 GDPR) for “online platforms” on their interfaces but does not explicitly refer to situations when these providers display OBA outside their platforms.<sup>1440</sup> In response to such ambiguity, supervisory authorities must provide appropriate guidance.

While the DSA and the DMA are potent tools for enforcing the EU legal framework for large platforms, and the UCPD acts as a general safety net protection for consumers, the GDPR provides comprehensive (substantive and enforcement) safeguards across the broadest range of digital service providers (Table 7-1). Nevertheless. The Article 29 Working Party (A29WP) opinion regarding OBA in

---

<sup>1438</sup> See *European Centre for Algorithmic Transparency*, EUROPEAN COMMISSION (2023), [https://algorithmic-transparency.ec.europa.eu/index\\_en](https://algorithmic-transparency.ec.europa.eu/index_en) (last visited Oct 26, 2023).

<sup>1439</sup> Morel et al., *supra* note 546.

<sup>1440</sup> Digital Services Act, *supra* note 2, 26 (3).

---

---

relation to personal data protection rules was issued in 2010 and is outdated.<sup>1441</sup> Therefore, it is recommended that the EDPB take charge of providing guidance on OBA.<sup>1442</sup> That being said, the EDPB must consult other supervisory authorities, including the European Commission, the EDSB, ECAT, and EAIB. It is recommended that the guidelines on OBA address at least the following issues:

- The extent to which consumer consent is valid if it is given in the “OBA-or-Pay” model to all digital service providers, but in particular to gatekeepers (section 6.3.1.1).
- The extent to which consumer consent is valid if (in the case of OBA via AdTech) there are numerous unknown vendors (section 6.3.1.2), and whether these vendors can rely on other Article 6(1)(a) GDPR legal grounds.
- In case consent to OBA results in a contractual relationship, how digital service providers can best communicate the “price” or the cost of such OBA contracts to consumers (section 6.3.1.3).
- Who is responsible, if anyone, for disclosing Article 26 (1) DSA information requirements to consumers when OBA is displayed by the “online platform” on the interface of a publisher other than this “online platform” through advertising networks (section 6.2.1).
- The extent to which publishers that are not “online platforms” within the definition of the DSA are required to disclose OBA-related information (e.g., required by Article 26(1) DSA), mainly when selling advertising space in AdTech open exchange (section 6.2.1).
- The requirements of digital service providers to comply with Article 8 GDPR and Article 28 (2) DSA prohibition with regards to OBA directed to minors, for example, regarding acceptable age verification tools that digital service providers can employ (section 6.2.2).
- Information requirements for VLOPs/VLOSEs to disclose in their advertising repositories, particularly in the context of Article 39 (2) (c) and (e) DSA requirements regarding the “payer” of advertising and the criteria. It is essential to clarify whether VLOPs/VLOSEs have to share information regarding behavioral personalization (i.e., “profiling”) and its criteria (section 6.4.1).
- The extent to which digital service providers are required to conduct a Data Protection Impact Assessment (DPIA) when processing personal data for OBA, particularly if via AdTech OBA (section 6.3.1.2).

---

<sup>1441</sup> ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 123 at 29.

<sup>1442</sup> Note that the DSA envisages the European Commission and the EDSB to provide guidance on many issues addressed in this section. Therefore, either of these bodies can alternatively take charge of issuing the general guidance on OBA, or broader online advertising. In such case, the EDPB has to be consulted closely. Lastly, if possible, these bodies should consider issuing joint guidelines.

- Adequate mitigation measures to address consumer manipulation risks of OBA in the context of VLOPs/VLOSEs and other digital service providers (section 6.4.3).

Addressing these issues can significantly support the enforcement of the EU legal boundaries for consumer manipulation via OBA. The enforcement of GDPR in practice has demonstrated that the OBA industry will leverage any legal ambiguity to challenge the boundaries of the EU legal framework until there is a binding decision from the enforcer or the CJEU.

### 7.3. Going Forward

Consumer manipulation is not limited to OBA-funded online environments but is also prevalent in online marketplaces, app stores, or video games.<sup>1443</sup> Evaluating consumer manipulation is a significant contribution because it is difficult to define, regulate, and enforce. However, digital service providers also exploit their consumers by coercing them, leading to harms similar to consumer manipulation. Meta’s announced move towards the “OBA-or-Pay” model to finance its platforms is an example of a coercive influence (section 6.3.1.1). Similar to interpersonal relationships, agents of exploitative influence can employ both manipulative and coercive actions at the same time and often change between forms of influence depending on the circumstances. Therefore, the central issue is the economic logic that results in asymmetries in information, power, and risk-bearing between digital service providers (particularly gatekeepers) and consumers.<sup>1444</sup> This economic logic enables and incentivizes the exploitation of consumer vulnerabilities.

Digital technologies and markets are evolving fast. Gatekeepers now deploy generative AI applications, such as Microsoft 365 Copilot,<sup>1445</sup> and extended reality (xR) devices, such as Apple Vision Pro<sup>1446</sup> and Meta Quest,<sup>1447</sup> to fundamentally change the way digital technologies mediate human experience in all aspects of individuals’ daily lives. Regardless of the plethora of threats associated with these technologies, the central challenge with them, as with OBA, is this economic logic and the asymmetrical relationship between consumers and companies that provide

---

<sup>1443</sup> See European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53.

<sup>1444</sup> See ZUBOFF, *supra* note 20. See also COHEN, *supra* note 28.

<sup>1445</sup> See Jared Spataro, *Introducing Microsoft 365 Copilot – Your Copilot for Work*, THE OFFICIAL MICROSOFT BLOG (2023), <https://blogs.microsoft.com/blog/2023/03/16/introducing-microsoft-365-copilot-your-copilot-for-work/> (last visited Sep 28, 2023).

<sup>1446</sup> See Apple Vision Pro, APPLE, <https://www.apple.com/apple-vision-pro/> (last visited Oct 26, 2023).

<sup>1447</sup> See Meta Quest Pro: Our most advanced new VR headset, META, <https://www.meta.com/nl/en/quest/quest-pro/> (last visited Jun 23, 2023).

them with digital products and services. With this in mind, this economic logic warrants attention from policymakers and academia going forward.

The proposed AI Act, when adopted, can significantly strengthen consumers' position in the digital market. Moreover, among other initiatives, the European Commission is considering the Digital Fairness Act (DFA) to provide digital consumers with appropriate protections,<sup>1448</sup> and there are growing calls to update the GDPR based on the lessons learned from its enforcement (“the GDPR 2.0.”).<sup>1449</sup> Nevertheless, enforcing the boundaries of the EU legal framework for OBA has revealed a weakness in the larger political economy that cannot be addressed by a singular legislative piece but by re-thinking digital industrial policy. In the transatlantic economic order, *neo-liberal* industrial policies have resulted in the rise of new private powers that undermine the same political freedoms that they used to emerge.<sup>1450</sup>

In EU law, *human dignity* marks the red lines within society, particularly concerning asymmetric power relationships.<sup>1451</sup> Threats to humanity from totalitarian regimes resulted in the affirmation of “citizen dignity” and threats from the industrialization of work – in “worker dignity”.<sup>1452</sup> In the age of surveillance capitalism, new threats to humanity come from private powers.<sup>1453</sup> These private powers are able to and have an incentive to benefit from exploiting their consumers through manipulative and coercive practices and, thus, can create market conditions that lead to social inequity and deterioration of overall quality of life.<sup>1454</sup> Therefore, the EU's commitment to human dignity as a foundational value requires an industrial policy to respond to surveillance capitalism by recognizing “consumer dignity”.

Such recognition of consumer dignity as a guiding principle of the EU industrial policy can ensure the protection of consumers in the face of digital asymmetries and allow digital transformation towards an increase in societal justice and overall quality of life. This requires that the academia and policymaker break the silos of different legal domains (e.g., public/private, human rights/competition) and create more coherence in the EU political-legal theory. The CJEU judgment in

---

<sup>1448</sup> See *Digital Fairness – Fitness Check on EU Consumer Law*, EUR. COMM'N (Sept. 10, 2022), [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en) (last accessed Feb. 12, 2023).

<sup>1449</sup> See Kai Zenner, *Fixing the GDPR: Towards Version 2.0*, DIGITIZING EUROPE (2021), [https://www.kaizenner.eu/post/gdpr\\_vol2](https://www.kaizenner.eu/post/gdpr_vol2) (last visited Oct 26, 2023).

<sup>1450</sup> See DE GREGORIO, *supra* note 154 at 2.

<sup>1451</sup> See DUPR, *supra* note 674.

<sup>1452</sup> See *Id.*

<sup>1453</sup> See ZUBOFF, *supra* note 20.

<sup>1454</sup> See about balancing asymmetries of power NASSIM NICHOLAS TALEB, *SKIN IN THE GAME*, 235-236 (2017).

the *Meta v Bundeskartellamt* case has planted a seed for such a coherent vision.<sup>1455</sup> The court's reasoning makes it evident that the gatekeeper power ends at the boundaries of consumer dignity in the EU, including in the digital realm.

Limiting digital markets by consumer dignity means recognition that consumers are, first and foremost, human beings, and, therefore, their freedom from (manipulative or coercive) exploitation takes priority over any gains in market efficiency and welfare.

---

<sup>1455</sup> Case C-252/21, *Meta v. Bundeskartellamt*, *supra* note 1017 at 117.