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

Zardiashvili, A.

CHAPTER 4. CONSUMER MANIPULATION VIA OBA

This thesis evaluates the ability of the European Union (EU) legal framework to safeguard against consumer manipulation harms of online behavioral advertising (OBA). Such an evaluation requires understanding ways in which OBA results in consumer manipulation. Chapter 3 builds an analytical framework for understanding manipulation, and Chapter 2 explains how OBA works. This chapter evaluates OBA from the analytical framework of manipulation developed in Chapter 3 and answers the third sub-question of the thesis:

SQ3: what is consumer manipulation via OBA?

In order to answer this question, this chapter is divided into four sections: Section 4.1 explains consumer manipulation in contexts of markets, online markets, and OBA, concluding that OBA involves manipulating consumers to extract attention, time, and data and that OBA involves manipulating consumers by personalizing advertising in a way to exploit consumer vulnerabilities. Section 4.2 addresses the manipulative extraction of attention, time, and data via OBA. Section 4.3 addresses the manipulative personalization of advertisements. Section 4.4 concludes by formulating an answer to SQ3 of this thesis.

4.1. Manipulation in Contexts

Manipulation can happen in a variety of contexts.[400] This thesis has illustrated some examples of interpersonal manipulation. *Intimate* relationships are contexts in which manipulation is prevalent.[401] Manipulation can also happen in a *political* context (section 1.4). As early as in Greek philosophy, manipulation was seen as a tool for politicians to sway the opinion of the masses.[402] Some forms of political philosophy regard manipulation as foundational to political organization.[403] Governments can also manipulate their citizens for social security and order ("social engineering", "state manipulation").[404] Manipulation can happen as *propaganda* or covert attempts to shape public opinion towards a particular issue.[405] This thesis evaluates manipulation in a particular context: Section 4.1.1. scopes manipulation in business-to-consumer commercial relationships (*consumer manipulation)*; Section 4.1.2. zooms in on consumer manipulation in the context of the online environment. Lastly, 4.1.3. further scopes the discussion of online consumer manipulation in the context of OBA.

4.1.1. Consumer Manipulation

In the market, manipulation has always been prevalent, mainly through attempts to influence consumers through manipulative advertising.[406] In an ideal market that maintains an equilibrium between production supply and consumer demand, businesses would use advertising and other marketing strategies to *inform* consumers about the availability of products and services that meet their

[400] *See* Coons and Weber, *supra* note 273, at 1.

[401] *See generally* Cave, *supra* note 338.

[402] *See* Noggle, *supra* note 265, at 1.2.

[403] *See generally* NICCOLÒ MACHIAVELLI, THE PRINCE (W. K. Marriott tran., eBook, 2006).

[404] *See e.g.,* Rogier Creemers, *China's Social Credit System: An Evolving Practice of Control*, (2018) https://papers.ssrn.com/abstract=3175792.

[405] *See e.g.,* YOCHAI BENKLER, ROBERT FARRIS & HAL ROBERTS, NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS (2018).

[406] Advertising about the availability of products and services took precedence as early as 4'000 BC when humans painted commercial communications on the walls. *See History of Advertising*, WIKIPEDIA (2023), https://en.wikipedia.org/w/index.php?title=History_of_advertising (last visited Feb 14, 2023). Advertising was normal in many civilizations of antiquity. For example, gladiator shows were advertised on the walls of Rome. *See* ERNEST S. TURNER, THE SHOCKING HISTORY OF ADVERTISING 6 (Rev. ed., 1965). The printing press allowed businesses to disseminate advertising to larger populations. People raised concerns about the manipulativeness of advertising from its outset. The earliest advertisements in the printing press in the sixteenth century included "quackery" – the promotion of alternative medicine for curing (often incurable) illnesses, which is regarded as a form of manipulative or fraudulent advertising today. *See Quackery*, BRITANNICA (2023), https://www.britannica.com/topic/quackery (last visited Feb 14, 2023). *See also* TURNER, *supra* note at 16.

preferences.[407] For example, a travel agency may advertise that it helps consumers plan their vacation, informing consumers who need help with planning about the availability of such a service. Moreover, consumers do not have rigid preferences but change daily (if not momentarily) depending on their circumstances and situations.[408] Therefore, by analyzing the overall market, businesses can anticipate consumer demand and use advertising to influence consumers' preferences.[409] For example, a travel agency can suggest taking a vacation in summer, or a lingerie store can recommend purchasing a Valentine's Day present for a partner. In summary, advertising facilitates the market by providing consumers with helpful information in the ideal scenario.[410]

Nevertheless, market practices do not always (if ever) reflect the ideal market scenario. Since the 1920s, the advertising industry has started relying on behavioral psychology insights, shifting the paradigm of understanding consumers from rational to malleable organisms that can be influenced toward suggested ends.[411] In one famous example, a toilet paper advertisement from 1931, a picture of a surgeon accompanied the slogan: "The trouble began with the harsh toilet tissue" – to associate toilet paper with rectal infections that may require surgical intervention.[412] As a result, marketers, incentivized to maximize *surplus value* (difference between the price paid and the actual market value) from the consumers or to create demand,

[407] Ideal market here reflects the perspective of welfare economics and allocative efficiency. *See* MASSIMO FLORIO & CHIARA PANCOTTI, APPLIED WELFARE ECONOMICS: COST-BENEFIT ANALYSIS OF PROJECTS AND POLICIES 32–62 (2 ed. 2022). For understanding advertising as communication of information, Floridi describes a following model: *Information* reduces uncertainty as answer does in relation to a question (*uncertainty*: what is the capital of France? *information*: capital of France is Paris). Having no answer to a question relates to having *uncertainty*. Having no question, relates to *ignorance* Floridi describes advertisement to be an information without preceding uncertainty, or an answer without a question. In other words, advertisement can be understood as "the information you have not asked for". *See* Lex Zard, *Online Targeted Advertising and Human Dignity: Prof. Floridi, Prof. Frischmann, Prof. Zuboff*, YOUTUBE 32:00-35:00 (2021), https://www.youtube.com/watch?v=WwXG4ZiKw6s (last visited Feb 13, 2023).

[408] *See* Merle Curti, *The Changing Concept of "Human Nature" in the Literature of American Advertising*, 41 BUS. HIST. REV. 335, 338 (1967).

[409] *See Supply and Demand*, BRITANNICA, https://www.britannica.com/topic/supply-and-demand (last visited Mar 1, 2023).

[410] *See* Robert Pitofsky, *Beyond Nader: Consumer Protection and the Regulation of Advertising*, 90 HARV. L. REV. 661, 663 (1977).

[411] In this particular context, this thesis refers to a branch of psychology that influenced the advertising industry from the 1920s to the 1950s: "behavioral psychology." John Watson, who coined the term "behavioral psychology," moved from academia to the advertising industry during this period. Since then, B.F. Skinner's "radical behaviorism" has a particular influence on advertising as well. *See generally* Bartholomew, *supra* note 85. Today, cognitive and social psychology, behavioral economics, and law fields also contribute to understanding consumer behavior and inform advertising practices. Therefore, this thesis considers these fields cumulatively "behavioral science."

[412] This advertisement was created by J.B. Watson – father of behavioral psychology. *See Id.,* 15.

started making exaggerated claims, and some even resorted to outright deception.[413] For example, since the mid-nineteenth century, the tobacco industry has advertised smoking (known to correlate to the high risk of lung disease) as a promising solution for lung health and offering better health overall.[414]

By the 1950s, when TVs were introduced to the mass audience, advertising started to be seen as "art" that entered its "golden age" (advertising expenditure in the U.S. amounted to several billion dollars annually).[415] Meanwhile, it was increasingly exposed that the advertising industry was targeting human decision-making vulnerabilities to exploit them and manipulate consumers through deception and pressure.[416] These revelations triggered a vigorous "consumer movement" that demanded balancing consumers' interests with the interests of businesses and subsequent consumer protection regulations in the 1960s and 1970s, primarily aimed to mitigate market failure risks by setting legal boundaries to manipulative advertising (section 6.1.1.).[417] While the empirical evidence about consumer responses to marketing communication was limited, and there was no consensus between industry and civil society about the psychology of consumer behavior, policymakers recognized advertising practices as a form of influence that could be manipulative and dangerous for the market (section 5.2.1.2.).[418]

In particular, consumer protection rules prohibited and closely regulated advertisements that outright *deceived* consumers by providing false information or otherwise *misled* consumers to have false beliefs, for example, by omitting certain information.[419] Similarly, while its effectiveness has been later debunked as a myth, *subliminal* advertising flashed in a millisecond and not perceptible to the consumer was also prohibited because it intended to influence consumers' preferences beyond

[413] *See* Pitofsky, *supra* note 410 at 666.

[414] One of the slogans promoted that "smoke not only checks disease but preserves the lungs". *See* A.V. Seaton, *Cope's and the Promotion of Tobacco in Victorian England*, 20 EUR. J. MARKETING 5 (1986). *See also* Staff Writers, *10 Evil Vintage Cigarette Ads Promising Better Health*, HEALTHCARE ADMINISTRATION DEGREE PROGRAMS (2013), https://www.healthcare-administration-degree.net/10-evil-vintage-cigarette-ads-promising-better-health/ (last visited Jun 30, 2023).

[415] *See generally* JIM HEIMANN, THE GOLDEN AGE OF ADVERTISING: THE 50S (TASCHEN's 25th anniversary special edition ed. 1999). *See also* ROBERT A. SOBIESZEK, THE ART OF PERSUASION: A HISTORY OF ADVERTISING PHOTOGRAPHY (1988). In the TV series Mad Men, Don Draper – creative director of the advertising agency in 1960s explains: "[a]dvertising is based on one thing: happiness. And do you know what happiness is? Happiness is the smell of a new car. It's freedom from fear. It's a billboard on the side of a road that screams with reassurance that whatever you are doing is ok. You are ok." *Mad Men: Smoke Gets Into Your Eyes* (Amazon Prime, 2007). *See also* JOHN A. HOWARD & JAMES HULBERT, *Advertising and The Public Interest: A Staff Report to the Federal Trade Comission* (1973).

[416] *See generally* VANCE PACKARD, THE HIDDEN PERSUADERS I-16-17 (1957).

[417] *See* Pitofsky, *supra* note 410, at 661.

[418] *See* Curti, *supra* note 408 at 353–358.

[419] *See* Hanson and Kysar, *supra* note 335 at 213.

their conscious awareness.[420] In contrast, policymakers did not find "puffery" – exaggerated affirmations of value, opinion, or praise about the product – manipulative to deserve regulatory intervention.[421]

In one famous example of the puffed campaign from the 1970s, *Coca-Cola* affirmed that its beverage was the "real thing" and "that's what the world needs".[422] Puffed commercial messages such as these were tolerated, partly because they had become a source of *entertainment* similar to music and cinema and somewhat because they facilitated economic growth in capital markets.[423] As a result, puffery became a standard in modern advertising. Moreover, the *Persuasion Knowledge Model (PKM)* developed in the 1980s suggested that as consumers became less sensitive to exaggerated claims (as well as misleading and deceptive practices that were retrospectively banned), they developed "schemer schema" or "persuasion knowledge" that equipped them with skepticism towards advertisements, making them aware of otherwise hidden influences.[424]

Since the 1990s, consumer protection enforcement has relied on the PKM to distinguish between mere puffery and misleading commercial messages.[425] Central to such evaluation was the benchmark consumer from whose perspective the manipulativeness of the advertisement was to judge. Historically, policymakers regarded consumers in the market as somewhat reasonable and only viewed them as vulnerable to manipulation if they belonged to a "labeled" vulnerable group, such as minors or people with mental disabilities.[426] However, behavioral science insights (section 3.2.1) about consumer biases have revealed that consumers who do not

[420] *See generally* Laura R. Salpeter & Jennifer I. Swirsky, *Historical and Legal Implications of Subliminal Messaging in the Multimedia: Unconscious Subjects*, 36 NOVA L. REV. 497 (2012).

[421] *See* Curti, *supra* note 408, at 338. For example, P.T. Barnum's extravagant advertisements were not considered misleading, because marketers expected consumers to appeal to reason, and not be influenced by such exaggerations. *See* Ivan L. Preston, *Regulatory Positions toward Advertising Puffery of the Uniform Commercial Code and the Federal Trade Commission*, 16 J. PUBLIC POL'Y MARKETING 336 (1997).

[422] Coke's brand manager, Ira C Herbert, identified the *need* in the young people for "the real, the original, and the natural". The fact that Coca-Cola was an original soda beverage was used to create a slogan: "Real life calls for real taste. For taste of your life – Coca-Cola". *The History of Coca-Cola's It's the Real Thing Sogan*, CREATIVE REVIEW (2012), https://www.creativereview.co.uk/its-the-real-thing-coca-cola/ (last visited Mar 2, 2023).

[423] *See* HOWARD AND HULBERT, *supra* note 415, at I–7.

[424] *See* Marian Friestad & Peter Wright, *The Persuasion Knowledge Model: How People Cope with Persuasion Attempts*, 21 J. CONSUMER RES. 1 (1994).

[425] Drawing a line between exaggerations and misleading advertising has been complicated for rule-makers and enforcers. Strategies and outcomes of this differ across different states and across the Atlantic. For example, in the prominent example where Apple advertised its iPhone 3G as "twice as fast for half the price", consumer acction against Apple has resulted in different U.S. and U.K. decisions. *See* Brian X. Chen, *Apple: Our Ads Don't Lie, But You're a Fool If You Believe Them*, WIRED, Dec. 2008, https://www.wired.com/2008/12/apple-says-cust/ (last visited Mar 2, 2023).

[426] *See* HOWARD AND HULBERT, *supra* note 415 at VI.

belong to pre-labeled vulnerable groups can be influenced by targeting biases shared by all human beings.

These revelations significantly altered how marketers influence consumers in ways that PKM could no longer capture.[427] Legal scholars have developed a "market manipulation" theory to explain practices marketers may use to exploit human decision-making vulnerabilities (e.g., cognitive biases) to bypass conscious deliberation even when the consumer is expected to treat information such as advertising with skepticism.[428] For example, investment performance is known not to disclose future performance in financial markets.[429] Nevertheless, financial firms sometimes advertise past performance with the disclaimer that "past performance does not guarantee future results".[430] This is targeted to exploit consumers' representativeness heuristic that mistakenly leads consumers to assume future results because of the stock's past performance.[431] In other examples, marketers may exploit the "irrelevant third option effect" (also the "decoy effect") that typically biases the consumer in favor of the options they initially disfavored.[432] For example, following the public outcry about the harmful effects of diet pills that contained ephedra, some manufacturers started to label their products as "ephedra-free", even though their supplements never contained ephedra, and, therefore, influenced consumers to perceive this option as "less risky".[433]

Updating consumer benchmarks in the EU consumer protection policy to reflect the behavioral insights in human beings has become one of the central issues and has also reached the Court of Justice of the EU (CJEU) (section 6.1.1).[434] This thesis

[427] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 21.

[428] "Market manipulation" has been coined in the series of studies published by Hanson and Kysar. *See* Hanson and Kysar, *supra* note 335. *See also* Jon Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: A Response to Market Manipulation*, ROGER WILLIAMS UNIV. L. REV. (2000). While Hanson and Kysar coin their theory as "market manipulation", the identical term also has a particular meaning in the criminal law context – that is, manipulation of stock prices that manipulates the market. Therefore, to avoid the confusion of this framing, this thesis refers to "consumer manipulation" to describe manipulation in the context of business-to-consumer commercial transactions.

[429] *See* Spencer, *supra* note 295, at 967.

[430] *See* Martin Brenncke, *The Legal Framework for Financial Advertising: Curbing Behavioural Exploitation*, 19 EUR. BUS. ORG. L. REV. 853 (2018).

[431] *See* Spencer, *supra* note 295, at 967.

[432] *See* Hanson and Kysar, *supra* note 335, at 1515.

[433] *See* Michael A. McCann, *Dietary Supplement Labeling: Cognitive Biases, Market Manipulation & Consumer Choice*, 31 AM. J. L. & MED. 215 (2014). *See also* Spencer, *supra* note 295 at 968.

[434] The Italian authority (Consiglio di Stato) has requested a preliminary ruling from the CJEU concerning whether the "new" behavioral discoveries about consumers' "bounded rationality" should be taken into account when considering average consumer benchmark. *See* Case C-646/22: Request for a preliminary ruling from the Consiglio di Stato (Italy) lodged on 13 October 2022 — Compass Banca

applies the analytical theory of manipulation built in Chapter 3 to understand the forms of influence that advertising practices belong to and their respective levels. Therefore, the business-to-consumer commercial practices that are hidden and targeted in a way that exploits decision-making vulnerabilities of *ordinarily vulnerable* consumers are considered *manipulative*.

4.1.2. Consumer Manipulation Online

Since the rise of the digital economy, consumer manipulation has become a topic of concern in online environments.[435] For example, in January 2023, the European Commission screened nearly a hundred online stores and found manipulative practices in almost half.[436] Moreover, since the early 2010s, the manipulative affordances of the Internet and other related technologies, such as AI, have been recognized as a new form of "digital market manipulation".[437] As a result of growing interest, by the 2020s, a comprehensive theory of "online manipulation" has emerged in academia.[438] These scholars broadly define online manipulation as the "use of information technology to covertly influence another person's decision-making," covering all manipulative practices facilitated via digital technologies.[439] This theory focuses not on a particular business model, economic logic, or market practice, such as OBA, but on the general characteristics of the internet that can exacerbate manipulation.[440]

The central premise of the online manipulation theory is that the online consumer is a *mediated* consumer.[441] They interact with businesses *through* the Internet. Authors compare the internet to eyeglasses in that once a person starts to use them, people usually forget they are wearing glasses unless something reminds them of them.[442] Similarly, online environments are designed to disappear from the conscious awareness of their users.[443] In other words, consumers focus on the content, such as messages, posts, and videos, instead of the medium that delivers it. Therefore, the Internet, in essence, is a see-through technology and particularly well-

SpA v. Autorità Garante della Concorrenza e del Mercato (CJEU) [hereinafter Compas Banca Request].

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

[436] *Manipulative Online Practices, supra* note 53.

[437] *See* Calo, *supra* note 38.

[438] *See generally* Susser, Roessler, and Nissenbaum, *supra* note 38. Spencer, *supra* note 295. THE PHILOSOPHY OF ONLINE MANIPULATION, *supra* note 74.

[439] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 29.

[440] Online manipulation as addressed by Susser, Roesller, and Nisseunbaum covers both commercial and political contexts. *See generally* Susser, Roessler, and Nissenbaum, *supra* note 38.

[441] *See* Calo, *supra* note 38 at 1003. *See* Susser, Roessler, and Nissenbaum, *supra* note 38. Spencer, *supra* note 295. THE PHILOSOPHY OF ONLINE MANIPULATION, *supra* note 74.

[442] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 33.

[443] *See* Mark Weiser, *The Computer for the 21 St Century*, 265 SCI. AM. 94 (1991).

placed for hidden influences.[444] However, in contrast to eyeglasses, the online environment is not only hidden but also easily *configurable – the* online environment can be easily adapted.[445] Therefore, due to its mediative and configurable nature, the Internet can exacerbate manipulation in two distinct but interrelated ways.

Firstly, as the Internet (and infrastructure that enables consumers to access and share content) remains in the background of consumer activities, it can be reconfigured to *extract* an unprecedented amount and variety of information.[446] Information about consumers has long been considered a valuable resource that can be leveraged to influence them.[447] However, while information about the consumer was once challenging to uncover, the internet makes very detailed information available almost at zero cost.[448] Consumers knowingly disseminate information about themselves online, such as pictures, posts, and search keywords.[449] Consumers also leave trails ("digital breadcrumbs" and "data exhaust"), such as how much time they spend looking at a particular offer (section 2.2.2).[450] Combining all information about them may reveal a great deal about their interests without consumers being aware of it – even tech-savvy consumers spend little time considering what is happening under the hood.[451] Such surveillance and information extraction ability can lead to businesses identifying consumers' *personal* decision-making vulnerabilities.[452] In one often-cited example, investigative journalists found that *Facebook* could identify when its teenage consumers felt "worthless" and

[444] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 33.

[445] *See* COHEN, *supra* note 28, at 38-47.

[446] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 30. *See also* ZUBOFF, *supra* note 20, at 63-98.

[447] Stigler writes: "One should hardly have to tell academicians that information is valuable: knowledge *is* power. However, it occupies a slum dwelling in the town of economics. Mostly it is ignored: the best technology is assumed to be know; the relationship of commodities to consumer preferences is a datum." George J. Stigler, *The Economics of Infrormation*, 69 J. POLIT. ECON. 213 (1961).

[448] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 31.

[449] *Id.* at 30.

[450] *See* ZUBOFF, *supra* note 20 at 68–69. *See also* Susser, Roessler, and Nissenbaum, *supra* note 38, at 30.

[451] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 33.

[452] *See* Zarsky, *supra* note 38, at 158-161. *See* Calo, *supra* note 38, at 1003. *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 29–31.

"insecure".[453] Moreover, internet surveillance can disclose new vulnerabilities by analyzing population-wide trends.[454]

Secondly, the online environment can be *hiddenly reconfigured* to target these identified personal or population-wide decision-making vulnerabilities.[455] The internet allows reconfiguration in real-time as a consumer interacts with the digital content and service and provides more information.[456] Moreover, it can be targeted narrowly to single out a specific individual.[457] Even when it is not deliberately targeted to exploit vulnerabilities, such narrow and information-rich algorithmic targeting can often lead to a manipulative effect.[458] Such algorithmic real-time adaptability of the online environment allows businesses to target consumers when and in which contexts consumers feel more vulnerable. In one such example, a marketing agency suggested targeting women with quick-fix beauty products on Mondays when they felt most unattractive.[459] For example, the most cited example of online manipulation is when Cambridge Analytica, a political consulting firm, used Facebook's advertising platform to promote campaigns for Brexit and US presidential candidate Donald Trump by targeting to exploit people's decision-making vulnerabilities.[460]

In sum, due to the mediative and configurative nature of the Internet and information technologies, there is a consensus in the state-of-the-art legal literature that consumers are *more than ordinarily vulnerable* to manipulation in the online environment, sometimes framing a baseline consumer online to have "digital

[453] Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless" [Updated]*, ARS TECHNICA, Jan. 5, 2017, https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/ (last visited Mar 3, 2023).

[454] *See* Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO. COMMC'N. & SOC'Y. 1, 6 (2016).

[455] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 32.

[456] *See* Yeung, *supra* note 454, at 6.

[457] *See generally* Marc Faddoul, Rohan Kapuria & Lily Lin, *Sniper Ad Targeting*, MIMS FINAL PROJ. (2019).

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

[459] The marketing study found that women felt less attractive on Monday mornings and, therefore, advised a marketing strategy promoting beauty products/fashion fixes on Monday mornings. *See* Rebecca J. Rosen, *Is This the Grossest Advertising Strategy of All Time?*, THE ATLANTIC, Oct. 2013, https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/ (last visited Feb 14, 2023).

[460] *See* Susser, Roessler, and Nissenbaum, *supra* note 38, at 9–12. In this case, targeting happened on personality traits that can be considered inherent and personal vulnerabilities. Furthermore, considering the information asymmetries in the case and the targeted situational vulnerabilities (e.g., uncertainty about the voting decision), targeted voters may have been at least highly vulnerable. Therefore, such targeting by Cambridge Analytica can be considered at least highly manipulative in the framework developed in this thesis.

vulnerability".[461] That being said, if "bounded rationality" insights of behavioral sciences suggest that all consumers, including offline, have a basic level of vulnerability that this thesis has framed as "ordinary vulnerability", digital vulnerability suggests a secondary layer of vulnerability, where consumers are more than ordinarily vulnerable.

There is further debate whether online manipulation is more likely when consumers access the Internet not via screens (e.g., personal computers, smartphones) but using extended reality (xR) devices such as Apple Vision Pro or Meta Quest Pro.[462] As Big Tech companies compete to facilitate xR technologies, it is essential to recognize that these devices further amplify the effects of the Internet on consumers with regards to their susceptibility to manipulation. It can be considered that xR consumers are not more than ordinarily vulnerable, but *highly vulnerable*.[463] Figure 4:1 illustrates these three layers of vulnerability in the vacuum devoid of other personal, relational, and situational layers: the first layer views "offline" consumers to be "ordinarily vulnerable". The second layer regards "online" consumers as having a layer of the situational vulnerability (being online) and views them as more than ordinarily "vulnerable". The third layer regards the consumers using xR to have additional situational vulnerability (using xR technologies) and views them as *highly vulnerable*.

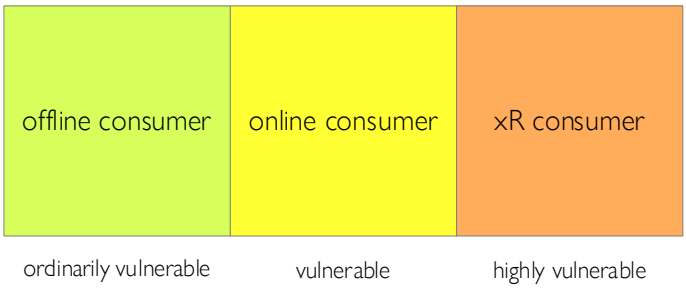

Figure 4:1. Levels of online consumer vulnerability (by author)[464]

Lastly, in the discussions of online manipulation, there has been a proliferation of studies about so-called "dark patterns" that focus on manipulative practices in

[461] *See generally* N. HELBERGER ET AL., *EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets*, (2021). *See also* N. Helberger et al., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, 45 J. CONSUM. POLICY 175 (2022); Davola and Malgieri, *supra* note 35; Federico Galli, *Digital Vulnerability*, *in* ALGORITHMIC MARKETING AND EU LAW ON UNFAIR COMMERCIAL PRACTICES 181, 181 (Federico Galli ed., 2022), https://doi.org/10.1007/978-3-031-13603-0_7 (last visited Mar 3, 2023).

[462] *See generally* EUROPEAN PARLIAMENT, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS DIRECTORATE-GENERAL FOR INTERNAL POLICIES, *Metaverse* (2023).

[463] *See* Zard and Sears, *supra* note 1, at 843.

[464] The figure is developed by the author based on Figure 3:2. Levels of Vulnerability (by Author).

online interface design and reverberate the paradigm focusing on the innate manipulativeness of the Internet.[465] Dark patterns can be defined as user interface patterns that steer, deceive, manipulate, or coerce consumers to take specific actions that may not be in their best interests.[466] While online manipulation and dark pattern literature provide a comprehensive overview of how businesses can exploit via the online environment, the problem with such framing is that they focus on manipulative features and not on the root causes of employing them online.[467] The online interface is typically deliberately designed to serve the purpose. While dark pattern literature often focuses on the designs, this thesis explores OBA as the purpose for implementing exploitative design features. Section 4.1.3 below builds upon the online manipulation and dark pattern literature and analyzes manipulative practices in the context of OBA. By doing this, this thesis intends to describe the root cause of most manipulative practices online.

4.1.3. Consumer Manipulation via OBA

Online manipulation and dark pattern literature successfully illustrate the manipulative potential of OBA's different aspects. However, they may mislead regulatory attention to focus on *symptoms* rather than directly addressing the root problem that gives way to such practices.[468] In particular, a more comprehensive analysis illustrates that the root problem is the economic logic through which digital content and services are monetized, often referred to as "surveillance capitalism" or "information capitalism."[469] This economic logic incentivizes providers of digital services and content to create an environment that increasingly influences consumers towards "guaranteed outcomes" for producing excess profit.[470] OBA infrastructure is the primary model that actualizes the economic logic of surveillance capitalism.[471] Therefore, reliance on OBA for monetizing online content and services can be seen as the primary cause of consumer manipulation in online environments.

---

[465] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 29–35.

[466] *See* M. R. Leiser, *Dark Patterns: The Case for Regulatory Pluralism Between the European Unions Consumer and Data Protection Regimes*, *in* RESEARCH HANDBOOK ON EU DATA PROTECTION LAW 240, 1 (2022). For different definitionsdefinitions of "dark patterns" *See* Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, *in* PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1 (2021), http://arxiv.org/abs/2101.04843 (last visited Feb 23, 2023).

[467] *See* Spencer, *supra* note 295.

[468] Spencer identifies this concern in "The Problem of Online Manipulation". *Id.* at 1002.

[469] *See* ZUBOFF, *supra* note 20. *See* COHEN, *supra* note 28.

[470] *See* ZUBOFF, *supra* note 20, at 93–97.

[471] *See* Zuboff, *supra* note 40 at 11–12. *See also* Cohen, *supra* note 22 at 14–29.

Consumer manipulation via OBA refers to situations when businesses facilitate or use OBA configuration or infrastructure in ways that hiddenly influence consumers either to give away their attention, time, and data or to act on a particular advertisement. Many studies evaluate some aspects of consumer manipulation via OBA. The manipulative design of cookie banners used by platforms or smaller publishers has been particularly closely studied.[472] Other studies focus on particular cases in which advertisers deliberately abuse the OBA infrastructure provided by large platforms or advertising intermediaries to influence singled-out consumers covertly.[473] For example, some studies address "sniper-targeting" methods in which advertisers (or their agencies) deliberately single out people to target them with manipulative advertising.[474] Nevertheless, analysis of consumer manipulation via OBA as the phenomenon at the heart of proliferating the Internet with manipulative practices is scarce.[475]

This thesis describes consumer manipulation via OBA and explains the phenomenon by expanding on two ways that OBA infrastructure leads to consumer manipulation.[476] First, section 4.2. expands on configuring the online environment to extract consumer attention, time, and data against consumers' genuine preferences. Second, section 4.3. expands on personalizing advertisements to influence consumers to act on them. In the end, section 4.4 connects two ways OBA leads to consumer manipulation and defines the essence of consumer manipulation via OBA. For both sections, this thesis relies on the analytical theory of manipulation developed in Chapter 3 to what extent these attempts to influence consumers are "manipulative".

4.2. Manipulative Extraction of Attention, Time, and Data

Online advertising monetizes consumer *attention* or "eyeballs".[477] The *time* consumers spend with publishers reveals where advertisers can reach the consumers online. OBA configuration introduces consumer *data* as the third essential element: publishers that allow OBA configuration follow an "extraction imperative" – they derive profit in proportion to which they increase consumer attention, time, and

[472] *See e.g.,* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 29-33.

[473] *See e.g.,* European Commission Study Recent Digital Advertising Developments, *supra* note 36, at 85–87.

[474] *See generally* Faddoul, Kapuria, and Lin, *supra* note 457.

[475] Strycharz and Duivenvoorde focus on exploitation not manipulation, personalization not behavioral personalization, and only on consumer protection law. *See* Strycharz and Duivenvoorde, *supra* note 361.

[476] In essence, all advertisement influences consumers in two stages: getting attention (e.g., "catching their ears", "turning their heads") and transmitting the information. *See* HOWARD AND HULBERT, *supra* note 415 at V–1.

[477] *See generally* WU, *supra* note 17.

data.[478] Therefore, having a solid financial incentive, publishers allowing OBA configuration design their online interfaces in a way that manipulate consumers to trap them, maximize their engagement, and maximize the amount of data they provide.

Section 4.2.1 describes manipulative practices publishers use to trap consumers with digital services and content and lists them in Table 4-1. Section 4.2.2 describes manipulative practices publishers use to maximize consumers' time and engagement with digital services and content and lists them in Table 4-2. Section 4.2.3 describes manipulative practices publishers and advertising intermediaries use to extract and maximize consumer data and lists them in Table 4-3. In this thesis, practices listed in Table 4-1, Table 4-2, and Table 4-4 are referred to as manipulative extraction practices ("MEP"s).

4.2.1. "Free" Internet

Many platforms and publishers provide their services and content to consumers without monetary payment, encouraging consumers to perceive these services and content as "free".[479] For example, until 2019, Facebook's sign-up page slogan was "It's free, and always will be".[480] Removing monetary payment is beneficial from the perspective of OBA, as it removes friction for new consumers to start using digital services and content.[481] Once consumers engage with digital services and content, their providers start collecting data about consumers and exposing them to advertisements. Due to the "free" nature of digital services and content, many consumers do not understand that value exchange is taking place. With this in mind, explicitly framing digital services and content as "free" and thus masking the fact that the commercial access-for-data bargain takes place can be regarded as a highly manipulative practice (*MEP1: free-framing*). Moreover, similar to active framing, not disclosing the access-for-data bargain to the consumers amounts to the same.

Moreover, platforms and publishers often remove other expressions of friction for consumers to start engaging with their services and content. For example, since 2019, Facebook has prided itself that "it's quick and easy" to create an account.[482] Indeed, consumers effortlessly access most digital services and content. In contrast, many publishers make it disproportionally tricky for consumers to cancel or deactivate their accounts or stop using their services or content. Such intentional asymmetry between signing up (that is easy) and canceling (that is difficult) is called

[478] *See* ZUBOFF, *supra* note 20, at 128–129. *See also* TRZASKOWSKI, *supra* note 41, at 10–12.

[479] *See* TRZASKOWSKI, *supra* note 41, at 12.

[480] Qayyah Asenjo & Alba Moynihan, *Facebook Quietly Ditched the "It's Free and Always Will Be" Slogan From Its Homepage*, BUSINESS INSIDER, Aug. 27, 2019, https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8 (last visited Feb 22, 2023).

[481] *See* TRZASKOWSKI, *supra* note 41 at 12.

[482] Asenjo and Moynihan, *supra* note 480.

"roach motel"[483] in the literature about dark patterns and is one of the most prevalent patterns in the online environment.[484] Roach motel pattern is often coupled with "trick questions" such as "Are you sure you would like to deactivate your account?" that can trigger consumers to second-guess their decisions, especially when they have already taken many steps towards deactivation (*MEP2: the roach motel*).[485]

The ease of accessing digital services and content is also reflected in "contracts" in the online environment, which generally take three forms:[486] (i) *click-wrap* contracts provide users with the notice of the "terms of service" that they need to scroll through and, in the end, the possibility to "accept" them; (ii) *modified click-wrap* contracts provide users with an "accept" button and a hyperlink that takes them to the "terms of service"; and (iii) *browse-wrap* contracts that provide notice of "terms of service" as a hyperlink somewhere in the app or the website, the consumer's agreement to which is merely implied by the digital content or the service provider (e.g., when visiting a website).[487] In click-wrap contracts, when terms of service are presented to the consumers, they rarely (if ever) read them because of the swaths of text.[488] Moreover, even when they read them, relevant

[483] "Roach Motel is an American brand of a roach bait device designed to catch cockroaches." Roach Motel, WIKIPEDIA (2022), https://en.wikipedia.org/w/index.php?title=Roach_Motel (last visited Feb 22, 2023).

[484] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 44.

[485] At the time of this writing, deactivating a Facebook account takes nine steps. It asks consumers for feedback when selecting the reason for deactivation, and, in the end, at the final step, it asks again if the user wants to deactivate the account. *See* Temporarily Deactivate Your Facebook Account, FACEBOOK HELP CENTER, https://www.facebook.com/help/214376678584711?helpref=faq_content (last visited Feb 22, 2023). Francien Dechesne pointed out to me that "roach motel" dark pattern also resemble "Hotel California" that is "programmed to receive" From where "you can check out any time you like; but you can never leave".

[486] *See* Zard and Sears, *supra* note 1, at 831.

[487] *See* CATERINA GARDINER, UNFAIR CONTRACT TERMS IN THE DIGITAL AGE 111 (2022). The terminology of "wrap" contracts comes from the "shrinkwrap" license agreement that was used for selling computer software. In the 1990s, software developers were contracting distributors, not the consumers, but wanted to bind end-users by the terms to mitigate litigation risks. The solution to this was the "end user license agreement' (EULA)", otherwise known as "shrinkwrap," because it entailed packaging the software in a plastic wrap that had terms printed on it. Terms explained that by purchasing software with such packaging, the end user was buying an option for software, not the software itself. Only by tearing the shrinkwrap were the consumers accepting the terms of service and entering into a contract with the software developers. "Click-wrap" agreements became common when sales shifted toward the online environment, where clicking "accept" to "terms and conditions" became an action similar to tearing the shrinkwrap. Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CALIF. L. REV. (1995).

[488] *See generally* Mark A. Lemley, *The Benefit of the Bargain*, Stanford Law and Economics Olin Working Paper No. 575 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4184946 (last visited Feb 23, 2023).

information, such as, for example, the fact that the publisher monetizes consumers' attention through OBA, is hidden in highly legalistic language, making it difficult for consumers to understand the nature of the exchange they enter (*MEP3: obscure legalese*).[489] In some cases, for example, when publishers rely on browse-wrap contracts, many consumers do not understand the access-to-attention bargain and do not even know they have entered a commercial relationship (*MEP4: covert contracts*).[490]

Moreover, *network effects* significantly affect how large platforms attract and maintain their users. To clarify, platforms of Alphabet and Meta have achieved a particularly significant gatekeeping position in the online environment – where most consumers access the open Web through their services (e.g., Google Search, Instagram).[491] Providing and improving services (e.g., web search, maps, and social interconnection) that consumers highly value is not a form of manipulation, and these services play a significant role in consumers staying with the platforms.[492] Nevertheless, these platforms can increase their "stickiness" by deliberate attempts to expand their reach over the internet and thwart other forms of networking.[493] For example, Alphabet and Meta enable consumers to use their accounts as "master accounts" to sign up and sign in on myriads of websites on the Web.[494] Such tools are manipulative when consumers are unaware that using them allows Alphabet and Meta to track further their online behavior, which is true in almost all cases (*MEP5: mastering*).[495] Section 4.2.3 elaborates on platforms' reach for data extraction.

Finally, all of the manipulative extraction practices listed above have in common that they hide their intentions. Highly legalistic text hides that the nature of exchange may be detrimental to consumers, and framing services as free hides the fact that consumers are in a commercial relationship. In a way, these practices resemble some of the practices adopted by the casinos, such as removing windows and clocks out of sight from gamblers and offering them unlimited amounts of food

[489] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 95–96.

[490] *See* TRZASKOWSKI, *supra* note 41, at 11–12.

[491] *See* Jean-Christophe Plantin et al., *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook*, 20 NEW MEDIA & SOC. 293 (2018).

[492] *See* COHEN, *supra* note 28, at 40–41.

[493] *Id.* at 41.

[494] *See* Plantin et al., *supra* note 491, at 301–307.

[495] Similarly, but outside of the OBA context, Google's use of reCAPTCHA can also be considered manipulative. The important aspect here is that most internet users do not know that Google uses user actions to improve their machine learning capabilities. As Google frames it: "reCAPTCHA makes positive use of this human effort by channeling the time spent solving CAPTCHAs into digitizing text, annotating images, and building machine learning datasets. This in turn helps preserve books, improve maps, and solve hard AI problems." *reCAPTCHA: Easy on Humans, Hard on Bots*, GOOGLE RECAPTCHA, https://www.google.com/recaptcha/intro/?hl=es/index.html (last visited Feb 23, 2023).

and alcohol only to keep them playing.[496] As described in Section 3.1.2, hiding intentions can be a method for manipulation (examples 8 and 9 in Figure 3:1). As concluded in Section 4.1.2., the online consumer is more than ordinarily vulnerable to manipulation (Figure 4:1). Understanding the online consumer this way, an influence with hidden intentions tailored to such vulnerable consumers can be regarded as *highly manipulative.* With this in mind, Table 4-1 categorizes mep1-mep5 as highly manipulative practices.

Table 4-1. Manipulative practices for attracting consumers (by author)

#	Name	Form and level of influence (Figure 3:3)
MEP1	*free-framing*	highly manipulative
MEP2	*the roach motel*	highly manipulative
MEP3	*obscure legalese*	highly manipulative
MEP4	*covert contracts*	highly manipulative
MEP5	*mastering*	highly manipulative

The adequate disclosure of otherwise hidden intentions can mitigate the manipulativeness of these practices. Additional layers of vulnerability can increase the manipulativeness of these practices. For example, if a business providing essential digital services to consumers (e.g., online search, social media) is a gatekeeper, there is another relational source of vulnerability, and thus, engaging in mep1-mep5 by gatekeepers can be considered extremely manipulative.

4.2.2. Maximizing Time

The idea of monetizing attention is not new nor unique to the digital economy.[497] For example, one early account of the attention economy from 1971 explains that:

> [I]n an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the *attention* of its recipients. Hence a *wealth of information* creates a *poverty of attention* and a need to allocate it efficiently among the overabundance of information sources that might consume it.[498](emphasis added)

[496] *See generally* NATASHA DOW SCHULL, ADDICTION BY DESIGN (2014).

[497] *See* TRZASKOWSKI, *supra* note 41, at 11.

[498] Herbert A. Simon, *Designing Organizations for an Information-Rich World*, *in* COMPUTERS, COMMUNICATIONS, AND THE PUBLIC INTEREST, 40–41 (1971).

The internet allows each individual almost unhindered access to the world's information.[499] This explains why search (Google Search in particular) has become the most valuable service online, as it provides users with *relevance* and, thus, the ability to manage their attention efficiently.[500] One way this relevance can be increased is by "recommender systems" that personalize digital content (section 2.2.2.). Like search engines, many other platforms rely on recommender systems to achieve relevance, improve the "user experience"(UX), and provide consumers with what *they* want to see.[501] This way, personalization has become the hallmark of modern-day digital services, where the most prominent platforms provide personalized entertainment (e.g., Netflix – personalized cinema, Spotify – personalized music).[502] Personalization can benefit consumers, as it can help them allocate their scarce attention more efficiently.[503]

However, such practices can influence consumers in salient ways, particularly if they remain hidden from consumers' awareness.[504] For example, if consumers are unaware that personalization takes place – they may act on a false premise that they are seeing what everyone else sees, and such perspective can be enough to affect their decisions (*MEP6: covert personalization of content*).[505] Moreover, content personalization, including and especially when it is hidden, can have far-reaching consequences: as many people receive their news and form opinions from social media platforms (e.g., Facebook, X), they may get locked into the "filter bubbles", that can amplify their opinions – giving way to more long-lasting behavior

[499] *See* TRZASKOWSKI, *supra* note 41, at 10.

[500] "Google's mission is to organize the world's information and make it universally accessible and useful". *See Google Mission*, GOOGLE SEARCH, https://www.google.com/search?q=google+mission (last visited Feb 23, 2023).

[501] TRZASKOWSKI, *supra* note 41, at 10. The internet usage in Europe has been dramatically increasing – according to Eurostat data, in 2022, 90% of EU27 individuals use internet, compared to 78% in 2015, and 67% in 2010. What did we use the internet for in 2022?, EUROSTAT, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20221215-2 (last visited Feb 23, 2023).

[502] Netflix claims to provide: "a personalized subscription service that allows our members to access entertainment content". *See Netflix Terms of Use*, *supra* note 140. Spotify: "personalized services for streaming music and other content". *See Terms and Conditions of Use*, SPOTIFY, https://www.spotify.com/uk/legal/end-user-agreement/ (last visited Feb 23, 2023).

[503] The European Commission study on manipulative personalization mystery shoppers disclosed that: "it was a common practice for large online companies to gather personal information to offer a 'personalised experience' to the user and that most people were used to it and did not find it problematic." *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 59.

[504] The European Commission study on manipulative personalization continues to illustrate that: "being conscious of the tracking and personalisation could have inhibited certain actions (e.g., commenting or sharing content), if consumers knew that this would have been recorded and used by the website/app." *See Id.*

[505] *Id.*

modification.[506] Potential consequences can also include moving consumers towards extreme fitness and dieting, radicalization, and misogyny (Chapter 5).

Secondly, personalization can become manipulative when practices do not stop merely at providing relevance for the consumers but are designed to maximize the time consumers spend with digital services and content.[507] This is particularly true when digital services or content are monetized through OBA because increased time spent with the service results in increased exposure to advertisements and, therefore, monetary profit.[508] The most illustrative example of such manipulative practices is designing an online interface with an endless feed that consumers can infinitely "scroll" (*MEP7: endless feed*).[509] This practice, one of the defining characteristics of video-sharing platforms (e.g., TikTok, Instagram), switches a path of least resistance towards continuing to use the service, making it easier to continue using the service than stop using it.[510]

Another widespread practice that similarly makes it easier to continue consuming the service and content is the *auto-play* function that many platforms employ that automatically continues providing content after initial consumption (*MEP8: auto-play*).[511] This can be, for example, when a new episode of TV series is automatically loaded on Netflix or another, often personalized, video is loaded on YouTube. Auto-play, infinite scroll, and personalization may be set as default modes by platforms, hiddenly influencing consumers towards maximizing the time they spend consuming their services and content and, thus, more exposure to advertisements (*MEP9: immersion selection*).[512]

Some platforms not only care about maximizing the time consumers spend on their services and content but also care about maximizing their engagement – how actively they interact with them, therefore designing their products with this aim.[513] For example, by notifying users that someone "liked" or "commented" on their content, platforms influence their consumers to associate their engagement, such as

[506] *See* ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2012). *See also* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 59.

[507] *See* TRZASKOWSKI, *supra* note 41, at 148–150.

[508] *Id.* at 11–12.

[509] *See e.g.,* Corina Cara, *Dark Patterns In The Media: A Systematic Review*, VII NETW. INTELL. STUD. 105. *See also* Mathur, Mayer, and Kshirsagar, *supra* note 466.

[510] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 37.

[511] *See* Aditya Kumar Purohit, Louis Barclay & A. Holzer, *Designing for Digital Detox: Making Social Media Less Addictive with Digital Nudges*, *in* CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2020), https://dl.acm.org/doi/abs/10.1145/3334480.3382810 (last visited Feb 23, 2023).

[512] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 64.

[513] *See* TRZASKOWSKI, *supra* note 41, at 12.

posts, tweets, videos, and images, with social validation (such notifications release the neurotransmitter dopamine), creating a positive reinforcement feedback loop that encourages consumers to maximize content sharing and engagement with the content (*MEP10: social validation loop*).[514] Many publishers "gamify" their services by, for example, providing their consumers with bonus points or other benefits (*MEP11: gamification*).[515] Many of these habit-forming ways publishers design their online interfaces are similar to mechanisms used in gambling slot machines that are addictive.[516]

Finally, these practices are often applied in combination and, at times, precisely target highly vulnerable people. For example, TikTok and Instagram have a large user base consisting of minors more vulnerable to manipulative practices than adults. When these practices are evaluated with the layered understanding of vulnerability proposed in this thesis (Figure 3:3), it can be concluded that they are *highly manipulative* when they are tailored to ordinarily vulnerable consumers. However, they can be *extremely manipulative* when directed toward highly vulnerable people. These practices can be *extremely manipulative* when used in xR devices.

Table 4-2. Manipulative practices for maximizing engagement (by author)

#	Name	Form and level of influence (Figure 3:3)
MEP6	*covert content personalization*	highly manipulative
MEP7	*endless feed*	highly manipulative
MEP8	*auto-play*	highly manipulative
MEP9	*immersion preselection*	highly manipulative
MEP10	*social validation loop*	highly manipulative
MEP11	*gamification*	highly manipulative

4.2.3. "Accept All" Data Extraction

Consumers' attention, time, and engagement can be measured by the *data* they leave behind when interacting with digital services and content.[517] Such "data exhaust" provides zero-cost information that publishers can use to improve their services and help consumers manage their time and attention more efficiently (optimizing for relevance).[518] In a way, processing such data can be "essential" for

[514] Ewafa, *Sean Parker - Facebook Exploits Human Vulnerability (We Are Dopamine Addicts)*, YOUTUBE (2017) https://www.youtube.com/watch?v=R7jar4KgKxs (last visited Feb 23, 2023). *See also* NIR EYAL, HOOKED: HOW TO BUILD HABIT-FORMING PRODUCTS (2014).

[515] *See generally* SCHULL, *supra* note 496.

[516] *See* TRZASKOWSKI, *supra* note 41, at 169.

[517] *See* ZUBOFF, *supra* note 20, at 68.

[518] *Id.* at 69.

improving the functionality of digital services (section 2.4.2.). However, as these data can also be used to infer consumers' interests and predict their future behavior, it is also a central *resource* for OBA (section 2.2.). Therefore, the OBA industry, led by the platforms that gatekeep access to the internet for consumers, sees consumer behavior data as the "raw material" that can be "mined" and "processed," similar to natural resources.[519]

However, extracting data from consumers' private experiences has particular legal boundaries. For example, in the EU, "personal data" that refers to data related to "an identified or identifiable living individual" is protected through a fundamental rights framework requiring that people *consent* to process data concerning them.[520] The OBA industry's initial attempts to monetize consumers' data without consent met with significant counter-reaction.[521] An amendment to the ePrivacy Directive in 2009 required users' consent to use cookies for collecting consumer data when their use was not strictly necessary.[522] Therefore, the OBA industry introduced the "cookie banners," asking consumers if they "accept" that the publisher processes their data for advertising.[523] Incentivized by the logic of surveillance capitalism to maximize data extraction, the industry primarily relied on the coercive tactic of *pre-ticking* consent boxes (i.e., "pre-selection"), which persisted until and shortly after the Court of Justice of the EU (CJEU) ruled in the *Planet49* case in late 2019 that this practice was illegitimate under the ePrivacy Directive and the General Data Protection Regulation (GDPR).[524]

---

[519] Data is often called to be "the new oil". *See* Joris Toonders Yonego, *Data Is the New Oil of the Digital Economy*, WIRED, Jul. 2014, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited Feb 24, 2023). *See also* ZUBOFF, *supra* note 20 at 81.

[520] CFREU, *supra* note 43, art. 8.

[521] For example, in 2004, Google announced that Gmail would scan the communications of the users for personalizing advertising placement. This raised issues with regard to consumer privacy. Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail, PRIVACYRIGHTS.ORG (Apr. 6, 2004), https://privacyrights.org/resources/privacy-and-civil-liberties-organizations-urge-google-suspend-gmail (last visited Feb 27, 2023). Consent is not the only legal ground for processing (section 5.1.1.). However, it is the most prominent basis that is explicitly highlighted in the text of the fundamental right to personal data protection. *See* Bart Custers et al., *The Role of Consent in an Algorithmic Society - Its Evolution, Scope, Failings and Re-Conceptualization*, *in* RESEARCH HANDBOOK ON EU DATA PROTECTION LAW 455 (2022).

[522] ePrivacy Directive, *supra* note 29, art. 5(3). The effective date in member states was generally in 2011, with a number of countries implementing the Directive several years later. European Law on Cookies, DLA PIPER (Nov. 27, 2020), https://www.dlapiper.com/en-gb/insights/publications/2020/11/european-law-on-cookies (last visited Jan 5, 2023). *See also* Zard and Sears, *supra* note 1, at 18.

[523] Cookie banners inform about both first and third-party cookies, as well as for other tracking technologies discussed in section 2.2.2.2. *See* Cristiana Santos et al., *Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens*, *in* PROCEEDINGS OF THE 20TH WORKSHOP ON WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 187 (2021), https://doi.org/10.1145/3463676.3485611 (last visited Feb 27, 2023).

[524] Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801.

In the 2010s, cookie banners also started to include other similarly coercive or manipulative tactics for extracting more data than the consumer intended.[525] Meta being particularly innovative in designing such practices on its platforms, they are often unified under the term "Privacy Zuckering," which pays homage to Meta's founder.[526] Moreover, in parallel with increasing legal demands, particularly after the *GDPR* and *Planet49* case, Consent Management Platforms (CMPs) have emerged to serve smaller publishers to acquire "compliant" consumer consent.[527] CMPs often boast of their capabilities for getting a high consent rate.[528] However, they often do this by directly targeting to exploit consumers' decision-making vulnerabilities.[529] As a result, in 2021, one study found that 89% of cookie banners were coercive or manipulative.[530] In summary, it is not far-fetched to argue that many CMPs provide publishers (and advertisers) with *manipulation-as-a-service*.

There are various ways in which advertising intermediaries, publishers, and CMPs, design cookie banners that can exploit consumers' decision-making vulnerabilities. For example, one *coercive* practice is not to offer an option to "reject" data processing on the first layer of the banner (instead, consumers may see "accept all" and "see cookie preferences").[531] Studies show that this practice significantly increased the likelihood of consent.[532] In the context of this thesis, this practice is *coercive* because it creates explicit friction and unequal paths between acceptance and rejection and, in a way, threatens a consumer to take away their *time* unless they accept data processing.[533]

On top of that, the second layer often includes even more coercive and manipulative practices.[534] In case a "reject" button is present, banners often employ a *manipulative* design. For example, "accept all" and "reject all" buttons may be

[525] *See* TRZASKOWSKI, *supra* note 41 at 165–167.

[526] Term "Privacy Zuckering" was coined by Tim Wu. *See* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2011). *See also* Mohit, *Privacy Zuckering: Deceiving Your Privacy by Design*, MEDIUM (Apr. 10, 2017), https://medium.com/@mohityadav0493/privacy-zuckering-deceiving-your-privacy-by-design-d41b6263b564 (last visited Feb 27, 2023).

[527] *See e.g.,* GDPR Compliant Consent Management, CIDAAS, https://www.cidaas.com/consent-management/ (last visited Feb 27, 2023). *See* Esther van Santen, *Cookie Monsters on Media Websites: Dark Patterns in Cookie Consent Notices*, *in* ICCGI 2022 - THE SEVENTEENTH INTERNATIONAL MULTI-CONFERENCE ON COMPUTING IN THE GLOBAL INFORMATION TECHNOLOGY (2022).

[528] *Quantcast Choice Powers One Billion Consumer consent Choices in Two Months Since GDPR*, QUANTCAST, https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/ (last visited Feb 27, 2023).

[529] *See* Leiser, *supra* note 466, at 245.

[530] *See* Santos et al., *supra* note 523, at 1.

[531] *See* EUROPEAN DATA PROTECTION BOARD, *Report of the Work Undertaken by the Cookie Banner Taskforce* 4 (2023).

[532] *See* Leiser, *supra* note 466, at 244.

[533] *See* EUROPEAN DATA PROTECTION BOARD, *supra* note 531, at 5.

[534] Case C-673/17, Planet49, 1 October 2019, ECLI:EU:C:2019:801., *supra* note 524.

presented differently in color or size, or an irrelevant third option may be introduced. Table 4-3 provides a non-exhaustive list of various manipulative and coercive practices used in cookie banners. Cookie banners practices identified as "manipulative" are further listed in Table 4-4.

Table 4-3. Exploitative patterns in cookie banners (by author)[535]

Name	Description	Analysis	Influence (Figure 3:3)
hidden tracking (MEP 12) [536]	A consumer is not presented with the notice about the data processing.	The processing of data is *hidden* from the consumer.	extremely manipulative
cookie wall[537]	A pop-up is a "wall" that consumers cannot close to access content unless they click "accept".	The only option to access the content is to accept data processing.	highly coercive
pre-ticked consent[538]	Pop-up presents an "accept" button and several options from which "accept all" is pre-selected	Friction – the consumer must change the default (unequal pathways).	coercive
no reject button[539]	A consumer is not presented with the "reject all" button on the first layer.	Friction – the consumer *must* choose to "see more" to reject (unequal pathways).	coercive
inaccurate classification (MEP 13)[540]	The consumer is presented with "accept all" or "accept only essential cookies," and data is inaccurately classified as *essential.*	Deceptive practice that exploits consumers' trust.	extremely manipulative

[535] This table (developed by the author) lists exploitative practices as identified in dark pattern literature. Analysis in the third column applies the framework developed in Chapter 3. Practices that are classified as "manipulative" are labeled as "mep"s.

[536] Hidden tracking is usually discussed under the "hidden information" category. Other forms include providing relevant information in a tiny font, or when the contrast ratio of the text compared to the background is too low. *See* van Santen, *supra* note 526, at 3.

[537] *See Id.*

[538] While pre-ticked consent boxes have decreased, such "preselection" dark patterns are still found in the cookie banners. *Id.*

[539] "No reject button" dark pattern is prevalent in cookie banners, that can be considered to be coercive. *See e.g.*, European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 109. *See also* EUROPEAN PARLIAMENT, POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC AND QUALITY OF LIFE POLICIES, *New Aspects and Challenges in Consumer Protection: Digital Services and Artificial Intelligence* 23 (2020). *See also* EUROPEAN DATA PROTECTION BOARD, *supra* note 531, at 4.

[540] *See* EUROPEAN DATA PROTECTION BOARD, *supra* note 531, at 7.

confusing grounds (MEP14)[541]	Consumers can accept and reject data processing on the grounds of "consent" and "legitimate interest" separately.	Consumers may think they need to refuse processing twice to not have their data processed for advertising.	extremely manipulative
false hierarchy (MEP15)[542]	"Accept All" and "Reject All" are presented differently in size.	Changing the choice environment to nudge consumers towards accepting all data processing.	highly manipulative
misdirection (MEP16)[543]	Accept All" and "Reject All" are presented differently in color, or color schemes are reversed.	It is the same as "false hierarchy" – a nudge towards accepting all data processing.	highly manipulative
irrelevant third option (MEP 17) [544]	Consumers are presented with "Accept All" and "Reject All" as well as the "Know More" button.	Exploits the irrelevant third-option bias ("decoy effect") that nudges a consumer to select more intrusive processing.	highly manipulative
no withdraw button[545]	Consumers are not presented with a button that allows them to withdraw consent in a similar way they accepted.	Significant friction to withdraw - the consumer must take several steps to withdraw consent.	coercive
OBA-or-Pay[546]	Consumers are required to pay unless they accept surveillance for OBA	Persuasiveness/coerciveness depends on the availability of alternatives (e.g., news sites). For gatekeepers, this model can create significant friction unless a third (free) alternative is provided.	coercive

Note that Table 4-3 classifies hidden tracking (MEP12), inaccurate classification (MEP13), and confusing grounds (MEP14) as *extremely manipulative* because of the assumption that online consumers exposed to these practices are *highly vulnerable*

[541] *Id.* at 6. van Santen, *supra* note 527 at 3.

[542] EUROPEAN DATA PROTECTION BOARD, *supra* note 531 at 6. van Santen, *supra* note 527 at 3.

[543] EUROPEAN DATA PROTECTION BOARD, *supra* note 531 at 6. van Santen, *supra* note 527 at 3.

[544] Author's contribution. Marieke van Hofslot, *Automatic Classification of Legal Violations in Cookie Banner Texts (Dissertation)*, Dec., 2022.

[545] EUROPEAN DATA PROTECTION BOARD, *supra* note 531 at 8.

[546] *See* Victor Morel et al., *Legitimate Interest Is the New Consent -- Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls*, (2023), http://arxiv.org/abs/2309.11625 (last visited Oct 12, 2023). "OBA-or-Pay" is sometimes called "consent-or-pay" or "pay-or-okay".

as they not only access the services online but also they legitimately expect that digital service providers comply with the privacy laws – expectation that is thwarted in case of these practices.

In most cases, each cookie banner contains more than one dark pattern – one study found that cookie consent notices contained, on average, 4.8 such patterns.[547] Also, if a consumer rejects cookies, this option is rarely recorded, and the publishers prompt the consumers to decide on data processing every time they visit (*MEP18: nagging*).[548] In contrast, if they accept, the cookies will be held on the consumers' computers for years, and consumers are not be prompted again.[549] Moreover, consumers are presented with a variety of banners that may deplete their egos and push them to, over time, give way to data processing.[550] Further, *framing* effects play a significant role: arguably, "accept all tracking" may more accurately represent an issue rather than accepting "cookies," which can have a connotation to a reward *(MEP19: framing effects*).[551]

In summary, publishers rely on manipulative practices to extract data from consumers in order to operationalize OBA configuration and infrastructure.[552] Such practices, listed in Table 4-4., include manipulative patterns in cookie banners that have become one of the defining characteristics of the online environment in the past decade. Even when, in rare cases, they provide seemingly neutral options to accept and reject data processing, consumers may remain unaware of exactly what data is being processed, by whom, and how it is used in advertising. In such cases, the mechanisms by which advertisements are shown to the consumers and how they are influenced remain hidden, raising concerns of manipulativeness in *advertising personalization,* which is further addressed in detail in section 4.3.

Table 4-4. Manipulative practices for data extraction (by author)

#	Name	Form and Level of Influence (Figure 3:3)
MEP12	*hidden tracking*	extremely manipulative
MEP13	*inaccurate classification*	extremely manipulative
MEP14	*confusing grounds*	extremely manipulative
MEP15	*false hierarchy*	highly manipulative

[547] van Santen, *supra* note 527 at 2.

[548] Zard and Sears, *supra* note 1 at 818.

[549] In some cases, the cookie retention period has been set for 8,000 years. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 224.

[550] *See* TRZASKOWSKI, *supra* note 41 at 197–202.

[551] *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 85–89.

[552] *Noyb* observes that the exploitative practices are decreasing. Nevertheless, a significant number of websites still incorporate such practices. *See Where did all the "reject" buttons come from?!*, NOYB (Oct. 27, 2022), https://noyb.eu/en/where-did-all-reject-buttons-come (last visited Feb 27, 2023).

MEP16	*misdirection*	highly manipulative
MEP17	*irrelevant third option*	highly manipulative
MEP18	*nagging*	highly manipulative
MEP19	*framing effects*	highly manipulative

4.3. Manipulative Advertisement Personalization

The ultimate goal of the manipulative extraction of attention, time, and data is to optimize online consumer interactions for maximizing consumer action on advertising, often measured by the *click-through rate* (CTR).[553] This goal is further expressed in the "prediction imperative," or the OBA configuration imperative that uses extracted data to algorithmically predict which advertisements the consumer is most likely to act on.[554] OBA infrastructure entails using artificial intelligence (AI) systems relying on vast datasets of consumer data to personalize advertisements.[555] Consumers may experience personalized advertisements as more relevant. Nevertheless, AI systems optimized to guarantee consumer action may also lead to advertisement personalization, exploiting consumers' decision-making vulnerabilities.[556] This section refers to the practices that may lead to consumer manipulation via advertising personalization as manipulative advertising practices. Section 4.3.1 describes and Table 4-5 lists manipulative advertising practices (referred to as "MAP" in the table) that may manipulate because they do not inform consumers of some essential aspects of advertising. Section 4.3.2 describes and Table 4-8 lists manipulative advertising practices that may manipulate consumers by exploiting their decision-making vulnerabilities.

4.3.1. Covert Personalization

Hiding the *commercial intent* of the communication or the fact that it is a sponsored advertisement has long been considered a manipulative practice.[557] Such hidden practices sometimes occur in the context of OBA within "native advertisements" that can disguise an ad by making it resemble the editorial content

[553] *See* ZUBOFF, *supra* note 20 at 95.

[554] Zuboff coins the term "economies of action" referring to the profitability of ensuring that consumers act on the advertisement. Economies of action is an ultimate economic aim. "Economies of scale" refer to extracting as much data as possible. "Economies of scope" refers to the extraction of as wide varieties of data as possible in many different contexts. Ultimately, the scope and scale of data serve the purpose of economies of action. The "prediction imperative" can be understood as the imperative that combines all of these three incentives. *Id.* at 199–202.

[555] *See* Judith Irene Maria de Groot, *The Personalization Paradox in Facebook Advertising: The Mediating Effect of Relevance on the Personalization–Brand Attitude Relationship and the Moderating Effect of Intrusiveness*, 22 J. INTERACT. ADVERT. 57 (2022).

[556] *See* ZUBOFF, *supra* note 20 at 212–218.

[557] *See* Friestad and Wright, *supra* note 424. *See also* FEDERAL TRADE COMMISSION, *.Com Disclosures: How to Make Effective Disclosures in Digital Advertising* (2013).

the consumer is accessing (*MAP1: hidden advertorial*).[558] Similarly, advertisements can also be disguised as search results (*MAP2: hidden paid ranking*).[559] In some contexts, such as TV advertisements, consumers may be able to discern communication as an advertisement, but in online environments, where consumers are more than ordinarily vulnerable to hidden influences (section 4.1.2), without explicit disclosure of commercial intent, practices can be considered *highly manipulative*.

When exposed to OBA infrastructure, consumers need more information than mere disclosure of commercial intent to become consciously aware of how an advertisement influences them.[560] The *Persuasion Knowledge Scale (PKS)* is one theoretical model that helps empirically analyze consumers' awareness of influence in their decision-making process.[561] By extrapolating PKS to OBA, this thesis argues that beyond the commercial intent, appropriate consideration of personalized advertisements requires consumers to evaluate information (1) that the personalization takes place, (2) about the criteria of personalization, (3) about who pays for personalized advertisement (e.g., advertiser), and (4) about the economic logic, including who performs the advertisement personalization (e.g., platform).[562]

Adopting PKS as a theoretical framework, advertisement personalization can be regarded as *hidden* and *manipulative* if any of these aspects of OBA are not disclosed to the consumer.[563] Firstly, understanding whether an advertisement is personalized is essential for the consumer to evaluate an ad.[564] Many consumers perceive personalized advertisements as advantageous.[565] They prefer personalized

[558] *See* for "native advertising" European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 31. *See also* Soontae An, Gayle Kerr & Hyun Seung Jin, *Recognizing Native Ads as Advertising: Attitudinal and Behavioral Consequences*, 53 J. CONSUM. AFF. 1421 (2019).

[559] Zard and Sears, *supra* note 1 at 811.

[560] Morey, Forbath, and Schoop find that in 2015 only 20% of the consumers who accepted data processing for personalization realized that they shared communication history, IP address, and web-surfing history for this purpose when using the standard web browsing. *See* Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARVARD BUSINESS REVIEW, May 2015, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (last visited Feb 28, 2023). *See also* CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 155. *See also* Boerman, Kruikemeier, and Zuiderveen Borgesius, *supra* note 81 at 269–270. *See* for digital vulnerability Helberger et al., *supra* note 461.

[561] *See* Sophie C. Boerman et al., *Development of the Persuasion Knowledge Scales of Sponsored Content (PKS-SC)*, 37 INT. J. ADVERT. 671 (2018). Boerman and others acknowledge that there is a research gap in understanding how consumers are influenced by the OBA. *See* Boerman, Kruikemeier, and Zuiderveen Borgesius, *supra* note 81 at 373.

[562] *See* about PKS in Boerman et al., *supra* note 561. Alternatively, Nissenbaum's framework of "contextual integrity" can also be applied. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

[563] *See also* Strycharz and Duivenvoorde, *supra* note 361 at 7.

[564] de Groot, *supra* note 555 at 57.

[565] Lee and Rha identify four consumer attitude groups about personalized advertising: (1) ambivalent – who perceive benefits and risks to be high, (2) privacy-oriented; (3) personalization-

and, thus, more relevant ads than random, unrelated marketing messages that they consider "spam".[566] However, identifying *covert* personalization significantly impacts consumers' perceptions of the advertising.[567] Multiple empirical studies have illustrated that consumers *feel* "vulnerable" when they encounter personalized advertisements they did not expect, for example, because they were unaware that their data was processed for this purpose.[568] In other words, consumers perceive ads as "intrusive", "creepy", and "annoying" when they find out that the advertisement was covertly personalized.[569]

Nevertheless, consumers do not always *accurately* identify personalization.[570] Algorithm-made inferences often elude consumers' conscious awareness mainly because they rarely (if ever) deliberately provide data used for personalization (section *2.1.3*.). For example, scrolling or mouse hovering behavior is rarely *deliberately* adopted to influence how ads are personalized.[571] Even when consumers are conscious that the OBA infrastructure uses data about their scroll/pause times for personalization, they cannot always accurately identify which advertisement relates to which scrolling pattern.[572] Therefore, unless explicitly disclosed that the advertisement is personalized, the practice remains hidden from the consumer and can be considered *highly manipulative* (*MAP3: covert ad personalization*).

Secondly, empirical evidence illustrates that while ad personalization disclosure increases consumers' trust in ads (and their likelihood to act on them), it does not

oriented; (4) indifferent group. They find that number of the ambivalent group is highest. *See* Jin-Myong Lee & Jong-Youn Rha, *Personalization–Privacy Paradox and Consumer Conflict with the Use of Location-Based Mobile Commerce*, 63 COMPUT. HUM. BEHAV. 453 (2016).

[566] de Groot, *supra* note 555 at 57.

[567] Elizabeth Aguirre et al., *Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness*, 91 J. RETAIL. 34, 43 (2015). Studies reveal that covert personalization decreases the likelihood of the consumer's acting on advertisements in cases when such covert personalization is discovered. These studies are mostly industry oriented, seeking to identify ways in which negative experiences of consumers (e.g., annoyance, frustration) can be minimized for more effective advertising personalization. *See e.g.,* Tobias Dehling, Yuchen Zhang & Ali Sunyaev, *Consumer Perceptions of Online Behavioral Advertising*, *in* 2019 IEEE 21ST CONFERENCE ON BUSINESS INFORMATICS (CBI) (2019), https://ieeexplore.ieee.org/document/8808011 (last visited Feb 28, 2023). *See also* Lee and Rha, *supra* note 566. de Groot, *supra* note 555.

[568] *See* Dehling, Zhang, and Sunyaev, *supra* note 567.

[569] *See* de Groot, *supra* note 555 at 62.

[570] *See* for *perceived* personalization and *actual* personalization in de Groot, *supra* note 555. *See* for European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 59.

[571] However, there are some instances when tech-savvy users of the social media try to "game" the algorithm by deliberately changing their scroll behavior (mostly for content filtering).

[572] *See* Alice Binder et al., *Why Am I Getting This Ad? How the Degree of Targeting Disclosures and Political Fit Affect Persuasion Knowledge, Party Evaluation, and Online Privacy Behaviors*, 51 J. ADVERT. The fact that consumers regard an influence as "intrusive", but they are not able to detect exactly how influence works can be seen as the example of manipulation.

always increase their understanding of how the influence works.[573] As a result, the OBA industry has increasingly adopted the *AdChoices* icon –  as a standard for ad personalization disclosure.[574] If consumers click these icons, they can get basic information about the criteria for personalizing the advertisement, such as broad demographic and contextual information (e.g., age, country of residence, language).[575]

Sometimes, the disclosure also includes the disclaimer that the advertisement is personalized with *other* information inferred based on the consumer's online behavior.[576] Nevertheless, such disclosure sometimes does not list *specific inferences* (e.g., interest in beauty products) nor *specific behavior* that inferences are drawn from (e.g. while scrolling paused on pictures of models).[577] However, such specific information about the inferences and behavior can be crucial for a consumer to understand the advertisers' strategy and, therefore, the nature of the influence.[578] Therefore, unless the criteria used for personalization are disclosed on the level of specific inferences and behavior connected to them, the practice can be considered *highly manipulative* (*MAP4: hidden criteria*).

The particularly challenging issue with regard to disclosing personalization criteria is that personalization algorithms can *implicitly* infer essential parameters.[579] For example, an algorithm (e.g., via a feat of lookalike audiences) can connect a consumer to other consumers with similar scrolling patterns that implicitly relate to their *anxiety* but explicitly are identified as "interest in self-help literature".[580] In this case, the disclosure will inform consumers that their scrolling behavior is similar to the scrolling behavior of others that expressed interest in self-help literature. Nevertheless, the fact that the behavior implicitly refers to these consumers' shared state of anxiety will remain hidden.[581] The issue is that making

[573] *See* Boerman, Kruikemeier, and Zuiderveen Borgesius, *supra* note 81 at 370.

[574] *Your Ad Choices* icon is an ad marker from the Digital Advertising Alliance (DAA) that has been established as an industry standard. *See YourAdChoices*, YOURADCHOICES, https://youradchoices.com/about (last visited Mar 1, 2023). *See also* Tami Kim, Kate Barasz & Leslie K John, *Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness*, 45 J. CONSUM. RES. 906 (2019).

[575] *See* Kim, Barasz, and John, *supra* note 574 at 910.

[576] *Id.* at 913.

[577] *See* European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 89. *See also* Kim, Barasz, and John, *supra* note 574. *See also* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 60.

[578] *See* Kim, Barasz, and John, *supra* note 574 at 917–918. *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 89.

[579] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUMBIA BUS. LAW REV. 494 (2019).

[580] Zard and Sears, *supra* note 1 at 811.

[581] *See* European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 89–90.

such implicit inferences *explicit* may be technologically unfeasible.[582] Nevertheless, without such disclosure, the influence remains *hidden*, and the practice – is *highly manipulative*. This is particularly important because most OBA relies on such inferences for interest-based targeting (section 2.2.2).[583]

Thirdly, it has always been essential for consumers to understand who is behind the advertisement – who is selling the product or the service.[584] Traditionally as well as in OBA, this entails the information about the advertiser and their advertising agency, and non-disclosure of who pays for the advertisement, such as an agency and an advertiser, can be considered a highly manipulative practice (*MAP5: hidden advertisers)*.

Fourthly and lastly, consumers must also understand economic logic or the model through which advertisement is monetized.[585] This can be challenging because OBA is a highly technical and dynamic infrastructure involving multiple parties that benefit from it (section 2.3.3). Without the information about who performs personalization and who benefits from it, influence stays hidden from consumer's conscious awareness.

Therefore, personalizing advertising without disclosing the information about the intermediaries involved and their respective roles in the process, practice can be considered *highly manipulative (MAP6: hidden infrastructure)*. Similarly, without disclosing every party between whom the information about the consumer was consolidated, personalization is *hidden* and, therefore, *highly manipulative (MAP7: hidden data sharing)*.

Table 4-5. Covert advertising personalization (by author)

#	Name	Form and level of Influence (Figure 3:3)
MAP1	*hidden advertorials*	highly manipulative
MAP2	*hidden paid ranking*	highly manipulative
MAP3	*hidden ad personalization*	highly manipulative
MAP4	*hidden personalization criteria*	highly manipulative
MAP5	*hidden advertisers*	highly manipulative
MAP6	*hidden infrastructure*	highly manipulative
MAP7	*hidden data sharing*	highly manipulative

[582] *See Id.*

[583] *See* Binder et al., *supra* note 573. *See also* Johann Laux, Sandra Wachter & Brent Mittelstadt, *Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice*, 58 COMMON MKT. L REV. 722 (2021).

[584] *See* HOWARD AND HULBERT, *supra* note 415 at IV. Friestad and Wright, *supra* note 424.

[585] *See* Boerman et al., *supra* note 561 at 674.

4.3.2. Targeting Vulnerability

Consumers can be manipulated via OBA when the *psychological mechanisms* ads use to influence them remain hidden.[586] Personalizing advertisements to target consumers' cognitive or psychological characteristics is called "psychological profiling" (also "psychological targeting").[587] Psychological profiling can involve targeting consumers' "personality traits" such as openness, conscientiousness, extraversion, agreeableness, and neuroticism (*OCEAN*).[588] Some empirical studies in consumer psychology have demonstrated targeting these traits as the most *effective* targeting practice.[589]

In contrast to the pre-digital era, the OCEAN traits can be inferred almost at zero cost in the online environment on a massive scale.[590] For example, they can be predicted from consumers' social media profiles,[591] language use,[592] and pictures.[593] Nevertheless, consumers' personality traits, in their essence, reveal the consumer's particular personal vulnerability, and in the context of OBA, they are highly vulnerable to the hidden influence.[594] Therefore targeting OCEAN traits can be considered an *extremely manipulative practice (MAP8: OCEAN targeting)*.

Psychological profiling can also involve targeting consumers' *affective states*, including their moods (e.g., sadness), emotions (e.g., surprise), stress levels (e.g., high-stress levels), and attachments (e.g., porn addiction).[595] These states can be predicted from consumers' spoken language,[596] keyboard typing patterns,[597] video

[586] *See* Strycharz and Duivenvoorde, *supra* note 361 at 7.

[587] *Id.*

[588] Sandra C Matz, Ruth E Appel & Michal Kosinski, *Privacy in the Age of Psychological Targeting*, 31 CURR. OPIN. PSYCHOL. 116 (2020).

[589] *See* Jacob B. Hirsh, Sonia K. Kang, & Galen V. Bodenhausen, *Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits*, 23 PSYCHOL. SCI. 578 (2012). *See also* Youngme Moon, *Personalization and Personality: Some Effects of Customizing Message Style Based on Consumer Personality*, 12 J. CONSUM. PSYCHOL. 313 (2002). *See also* Barbara K. Rimer & Matthew W. Kreuter, *Advancing Tailored Health Communication: A Persuasion and Message Effects Perspective*, 56 J. COMMC'N. S184 (2006).

[590] *See* Matz, Appel, and Kosinski, *supra* note 588.

[591] *See* Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NATL. ACAD. SCI. 5802 (2013).

[592] *See* Gregory Park et al., *Automatic Personality Assessment Through Social Media Language*, 108 J. PERS. SOC. PSYCHOL. 934 (2015).

[593] *See* Crisitina Segalin et al., *The Pictures We Like Are Our Image: Continuous Mapping of Favorite Pictures into Self-Assessed and Attributed Personality Traits*, 8 IEEE TRANS. AFFECT. COMPUT. 268 (2017).

[594] *See* Strycharz and Duivenvoorde, *supra* note 361 at 7.

[595] *See* Matz, Appel, and Kosinski, *supra* note 588 at 117.

[596] *See* Tuka AlHanai & Mohammad Ghassemi, *Predicting Latent Narrative Mood Using Audio and Physiologic Data*, 31 PROC. AAAI CONF. ARTIF. INTELL. (2017), https://ojs.aaai.org/index.php/AAAI/article/view/10625 (last visited Mar 7, 2023).

[597] *See* Spencer, *supra* note 295 at 979.

data,[598] and metadata.[599] Targeting consumer affect states, sometimes called "dynamic emotional targeting" or "emotion analytics," has been a prevalent practice in the OBA industry.[600] Hiddenly targeting someone's affective states can exploit their situational vulnerabilities and, therefore, can be considered an *extremely manipulative practice* (*MAP9: affect targeting*).[601] Similarly, *personal hardships* can be a form of consumers' situational vulnerability that businesses can exploit.[602] Table 4-6 provides a non-exhaustive list of personal hardship examples that can be exploited, and therefore, targeting of which can be considered *extremely manipulative* (*MAP10: hardship targeting*).

Table 4-6. Hardship targeting (from Google Ad Policy) [603]

MAP10: hardship targeting	*examples of personal hardships*
10.1. physical illness	physical injury, arthritis, diabetes;
10.2. mental health	anxiety disorders, attention hyperactivity deficit disorder (ADHD);
10.3. sexual health	erectile dysfunction, sexually transmitted diseases (STDs), infertility;
10.4. financial difficulties	negative credit score, insolvency;
10.5 relationship-related	going through a divorce, considering breaking up; [604]
10.6. trauma or grief	experienced domestic abuse, loss of a loved one;

Advertisements can be personalized based on consumers' personality traits, affective states, personal hardships, and particular *idiosyncrasies* or *cognitive styles*.[605] Profiling a consumer as having characteristics and styles such as being

[598] *See* Thales Teixeira, Michel Wedel & Rik Pieters, *Emotion-Induced Engagement in Internet Video Advertisements*, 49 J. MKTG. RES. 144 (2012).

[599] *See* Robert LiKamWa et al., *MoodScope: Building a Mood Sensor from Smartphone Usage Patterns*, *in* PROCEEDING OF THE 11TH ANNUAL INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS, AND SERVICES 389 (2013), https://doi.org/10.1145/2462456.2464449 (last visited Mar 7, 2023).

[600] *See The power of emotion analytics*, THINK WITH GOOGLE, https://www.thinkwithgoogle.com/intl/en-154/marketing-strategies/data-and-measurement/emotion-analytics-powerful-tool-augment-gut-instinct/ (last visited Mar 7, 2023). *See also* The Power of Emotional Targeting in Advertising, THEVIEWPOINT (2021), https://theviewpoint.com/insights/blog/the-power-of-emotional-targeting-in-advertising/ (last visited Mar 7, 2023). *See also* Spencer, *supra* note 295 at 979.

[601] Strycharz and Duivenvoorde, *supra* note 361 at 18.

[602] *See* Personalized Advertising, *supra* note 120.

[603] *See* examples of hardship targeting that is restricted to advertisers by Google *Id*.

[604] Personalization can also happen to differentiate prices in a way that some (often more loyal) consumers are charged more for similar products. Advertising differentiated prices can be considered OBA, and be regarded manipulative unless such personalization is disclosed. *See* European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 40. Sears, *supra* note 80.

[605] *See* Calo, *supra* note 38 at 1017.

"impulsive", a "natural follower", or a "scarcity-phobic" is called "persuasion profiling".[606] Personalizing advertisements following such persuasion profiles can be rephrased as personalization that targets to exploit consumers' decision-making vulnerabilities and, therefore, is, in essence, another *extremely manipulative practice* (*MAP11: persuasion profiling*). A consumer's belief system can act as a particular decision-making vulnerability that manipulators can exploit (section 3.2.2).[607] Therefore, personalizing advertisements based on consumers' beliefs or identities can be extremely manipulative (*MAP12: identity targeting*). *Table 4-7* provides a non-exhaustive list of identities targeting which can be considered manipulative:

Table 4-7. Targeting identity (from Google Ad Policy, examples added)[608]

MAP12: identity targeting	*examples of categorizing identities*
12.1. sexual orientation	interested in dating same-sex, lgbtq+ community;
12.2. political ideology	climate change activist, Republican;
12.3. trade union membership	taxi driver;
12.4. race or ethnicity	Caucasian, Hispanic/LatinX;
12.5. religious beliefs	Mormon church, Muslim;
12.6. marginalized groups	refugees, indigenous people, transgender identity;

Advertisers can use the affordances of OBA to exploit consumers' decision-making vulnerabilities. One such affordance is the ability of OBA to micro-target so narrowly to single out an individual consumer, enabling "segment-of-one marketing".[609] Usually, advertisers use microtargeting criteria to define their audiences, but at times, they can also exploit the criteria to reach a *pre-defined* consumer segment that can be a single individual.[610] Such exploitation of OBA by the advertisers is called "sniper ad targeting", and one of its main goals is to manipulate *(MAP13: sniper ad targeting*).[611]

In one quintessential example, John Jones used sniper ad targeting to manipulate his wife, friends, and relatives to change their religious beliefs.[612] He came across the information about the controversies about the Mormon Church and

[606] *See generally* KAPTEIN MAURITS, PERSUASION PROFILING: HOW THE INTERNET KNOWS WHAT MAKES YOU TICK (2015).

[607] *See* Noggle, *supra* note 265.

[608] *See* Personalized Advertising, *supra* note 120.

[609] Faddoul, Kapuria, and Lin, *supra* note 457; EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, *supra* note 53 at 33.

[610] *See* Faddoul, Kapuria, and Lin, *supra* note 457 at 6.

[611] *Id.* at 4.

[612] *Id.*

was convinced to leave it.[613] However, when he systematically failed to convince his wife and relatives to read the same information, he created a *MormonAds* campaign and leveraged his knowledge of OBA to single out his wife, friends, and the larger community – having a life-altering impact on everyone involved.[614]

Manipulation via OBA can be deliberate, as in the case of sniper ad targeting, but it can also happen "carelessly" when an advertiser or advertising intermediary neglects that an algorithm can exploit consumers' decision-making vulnerability.[615] This can, for example, occur when the consumer is targeted based on "lookalike" or "similar" audiences (section 4.3.1). In such cases, an algorithm may process data about keyboard typing patterns and does not explicitly identify that such a pattern relates to the person experiencing anxiety and, therefore, targets the consumer's decision-making vulnerability. Empirical research could reveal whether it is possible to make such implicit inferences visible, but otherwise, until this is so, these practices can be considered extremely manipulative (*MAP14: lookalike audiences*).

Personalizing advertising can be considered *extremely manipulative* if it targets people otherwise vulnerable to manipulation in the online environment. In particular, it is often argued that when targeted with personalized advertising, children may not fully understand the nature of influence and, therefore, are more likely to be manipulated (*MAP15: targeting minors*).[616] In addition, OBA personalization can have similar effects when targeted at the elderly (*MAP16: targeting elderly*) and consumers with cognitive disabilities (*MAP17: targeting disabilities*).

Finally, publishers sometimes use coercive dark patterns to ensure the consumer remains exposed to advertising personalization. For example, a prevalent coercive practice is to make pre-select advertising personalization a default.[617] Similarly, threatening with irrelevant content or dysfunctional service when the consumer considers choosing against advertisement personalization can be a coercive practice.[618] Some dark patterns are increasingly personalized and tailored

[613] *See* Kevin Poulsen, *Inside the Secret Facebook War For Mormon Hearts and Minds*, THE DAILY BEAST, Feb. 10, 2019, https://www.thedailybeast.com/inside-the-secret-facebook-war-for-mormon-hearts-and-minds (last visited Mar 7, 2023).

[614] *See* Faddoul, Kapuria, and Lin, *supra* note 457 at 4.

[615] *See* Klenk, *supra* note 305.

[616] van der Hof Simone & Eva Lievens, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*, 19 (2017), https://papers.ssrn.com/abstract=3107660 (last visited Mar 8, 2023). *See also* Valerie Verdoodt & Eva Lievens, *Targeting Children with Personalised Advertising : How to Reconcile the (Best) Interests of Children and Advertisers*, *in* DATA PROTECTION AND PRIVACY UNDER PRESSURE : TRANSATLANTIC TENSIONS, EU SURVEILLANCE, AND BIG DATA 313 (2017).

[617] FORBRUKERRADET, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy* 44 (2018).

[618] *Id.*

to manipulate or coerce each consumer based on their vulnerabilities, causing more significant legal and policy concerns.[619]

Table 4-8. Advertising practices that exploit vulnerabilities (by author)

#	Name	Formand level of influence (Figure 3:3)
MAP8	*OCEAN targeting*	extremely manipulative
MAP9	*affect targeting*	extremely manipulative
MAP10	*hardship targeting*	extremely manipulative
MAP11	*persuasion profiling*	extremely manipulative
MAP12	*identity targeting*	extremely manipulative
MAP13	*sniper ad targeting*	extremely manipulative
MAP14	*lookalike audiences*	extremely manipulative
MAP15	*targeting minors*	extremely manipulative
MAP16	*targeting elderly*	extremely manipulative
MAP17	*targeting intellectual disabilities*	extremely manipulative

4.4. Conclusion: Consumer Manipulation via OBA

This section summarizes Chapter 4 to answer the second sub-question of the thesis:

SQ3: what is consumer manipulation via OBA?

This thesis defines consumer manipulation via OBA as manipulation occurring due to digital service providers executing or facilitating OBA configuration and infrastructures. In other words, consumer manipulation via OBA refers to the situation when 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.

Within the framework of manipulation developed in this thesis, digital service providers can be said to exert a manipulative influence if they hide and if they deliberately target to exploit consumer vulnerabilities or disregard that their OBA practices, including any AI system that they deploy, are likely to exploit consumer decision-making vulnerability. Table 4-9 provides a list of manipulative OBA practices identified in this thesis that is non-exhaustive.

[619] *See European* Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 60.

Table 4-9. Manipulative practices of OBA (by author)

#	Name	Form of level of influence (Figure 3:3)
MEP1	*free-framing*	highly manipulative
MEP2	*roach motel*	highly manipulative
MEP3	*obscure legalese*	highly manipulative
MEP4	*covert contracts*	highly manipulative
MEP5	*mastering*	highly manipulative
MEP6	*covert personalization*	highly manipulative
MEP7	*endless feed*	highly manipulative
MEP8	*auto-play*	highly manipulative
MEP9	*immersion preselection*	highly manipulative
MEP10	*social validation loop*	highly manipulative
MEP11	*gamification*	highly manipulative
MEP12	*hidden tracking*	extremely manipulative
MEP13	*inaccurate classification*	extremely manipulative
MEP14	*confusing grounds*	extremely manipulative
MEP15	*false hierarchy*	highly manipulative
MEP16	*misdirection*	highly manipulative
MEP17	*irrelevant third option*	highly manipulative
MEP18	*nagging*	highly manipulative
MEP19	*framing effects*	highly manipulative
MAP1	*hidden advertorials*	highly manipulative
MAP2	*hidden paid ranking*	highly manipulative
MAP3	*hidden ad personalization*	highly manipulative
MAP4	*hidden personalization criteria*	highly manipulative
MAP5	*hidden advertisers*	highly manipulative
MAP6	*hidden network*	highly manipulative
MAP7	*hidden data sharing*	highly manipulative
MAP8	*OCEAN targeting*	extremely manipulative
MAP9	*affect targeting*	extremely manipulative
MAP10	*hardship targeting*	extremely manipulative
MAP11	*persuasion profiling*	extremely manipulative
MAP12	*identity targeting*	extremely manipulative
MAP13	*sniper ad targeting*	extremely manipulative
MAP14	*lookalike audiences*	extremely manipulative
MAP15	*targeting minors*	extremely manipulative
MAP16	*targeting elderly*	extremely manipulative
MAP17	*targeting persons with disabilities*	extremely manipulative

As can be seen in Table 4-9, this thesis identified 19 manipulative extraction practices (MEPs) and 17 manipulative advertising practices (MAPs). This thesis classifies 16 MEPs (1-11, 15-19) as highly manipulative and 3 MEPs (12-14) as extremely manipulative. Similarly, this thesis classifies 7 MAPs (1-7) as highly manipulative and 10 MAPs (8-17) as extremely manipulative. Such classifications are based on the evaluation of different vulnerability levels of the consumers according to the framework developed in section 3.3.3. Such classification is meaningful - highly manipulative practices tend to be forms of exploitation when hidden aspects of the influence are eliminated by their disclosure. In contrast, extremely manipulative practices continue to be exploitative even if the influence is overt. Then, they can be classified as forms of coercive influence. For example, in case digital service providers disclose to the consumers that OBA targets their emotional state, such advertising can be considered coercive and exploitative.