



Universiteit
Leiden
The Netherlands

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

Zardiashvili, A.

Citation

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

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

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

POWER & DIGNITY

*The Ends of Online Behavioral Advertising
in the European Union*

LEX ZARD



LEIDEN UNIVERSITY

POWER & DIGNITY

*The Ends of Online Behavioral Advertising
in the European Union*

POWER & DIGNITY

The Ends of Online Behavioral Advertising in the European Union

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 7 mei 2024
klokke 16.15 uur

door

ALEKSANDRE ZARDIASHVILI

geboren te Tbilisi (Georgië)

in 1992

Promotoren: Prof.mr.dr.ir. B. H.M. Custers
Prof.dr.mr. S. van der Hof

Co-promotor: Dr. F. Dechesne

Promotiecommissie: Prof.mr.dr. B.W. Schermer
Prof.dr.mr. V. Mak
Dr. G. Malgieri
Prof.dr. S. Zuboff (Harvard University, Boston, USA)
Prof.mr. F.J. Zuiderveen Borgesius (Radboud Universiteit)

Copyright © by Aleksandre Zardiashvili, 2024
All rights reserved
ISBN 978-94-6473-432-4, Lex Zard.
Printed by *IPSKAMP printing*, Enschede, the Netherlands



**Universiteit
Leiden**
The Netherlands

for joy

TABLE OF CONTENTS

LIST OF FIGURES	XI
LIST OF TABLES	XII
ACRONYMS	XIII
CHAPTER 1. INTRODUCTION: POWER & DIGNITY	1
1.1. Setting the Stage	1
1.2. Research Questions	8
1.3. Methodology	9
1.4. Scope	12
1.5. Structure	13
CHAPTER 2. ONLINE BEHAVIORAL ADVERTISING	16
2.1. The OBA Paradigm	17
2.1.1. Targeting	17
2.1.2. Behaviorism	18
2.1.3. The Internet.....	19
2.2. The OBA Configuration	21
2.2.1. Online Targeted Advertising.....	21
2.2.2. Profiling: Behavioral Personalization	23
2.3. The OBA Markets	25
2.3.1. Publishers and Advertisers.....	26
2.3.2. Walled Gardens and AdTech	27
2.3.3. Markets and Power.....	30
2.4. The OBA Infrastructures	32
2.4.1. Real-Time Bidding (RTB)	33
2.4.2. Cookies and Mobile IDs.....	35
2.4.3. Cookieless OBA.....	38
2.5. Conclusion: Online Behavioural Advertising	41
CHAPTER 3. MANIPULATION	43
3.1. Influencing Human Behavior	44

3.1.1. Influence.....	44
3.1.2. Persuasion, Coercion, and Manipulation.....	45
3.1.3. Manipulation: Hidden, Successful, Intentional Influence.....	50
3.2. Methods: Exploitation of Vulnerability	52
3.2.1. Cognitive Biases	53
3.2.2. Beliefs, Desires, Emotions, and Nudges	55
3.3. Measuring Manipulativeness	58
3.3.1. Vulnerability	59
3.3.2. Levels of Vulnerability	61
3.3.3. The Spectrum of Influences	65
3.4. Conclusion: Manipulation	67
CHAPTER 4. CONSUMER MANIPULATION VIA OBA	69
4.1. Manipulation in Contexts	70
4.1.1. Consumer Manipulation.....	70
4.1.2. Consumer Manipulation Online.....	75
4.1.3. Consumer Manipulation via OBA	79
4.2. Manipulative Extraction of Attention, Time, and Data.....	80
4.2.1. “Free” Internet.....	81
4.2.2. Maximizing Time.....	84
4.2.3. “Accept All” Data Extraction.....	87
4.3. Manipulative Advertisement Personalization.....	93
4.3.1. Covert Personalization	93
4.3.2. Targeting Vulnerability.....	98
4.4. Conclusion: Consumer Manipulation via OBA.....	102
CHAPTER 5. CONSUMER MANIPULATION HARMS OF OBA.....	105
5.1. Theories of Harm	106
5.1.1. Consumer Manipulation Harms	106
5.1.2. Welfare: Free Market Approach	109
5.1.3. Dignity: Human Rights Approach	113
5.1.4. Unifying Strands: Capability Approach.....	119
5.2. Typology of Consumer Manipulation Harms.....	122

5.2.1. Economic Harms	123
5.2.1.1 Economic Loss: Personal Detriment	123
5.2.1.2 Market Harms: Structural Detriment	124
5.2.2. Environment Harms	130
5.2.3. Affinity Harms	132
5.2.4. Privacy Harms	133
5.2.5. Authenticity Harms	134
5.2.6. Integrity Harms	136
5.2.7. Dignity Harms	137
5.2.7.1 Threat to Children	139
5.2.7.2 Threat to Democracy	140
5.2.7.3 Threat to Vulnerability	141
5.3. Conclusion: Consumer Manipulation Harms of OBA	143
CHAPTER 6. BOUNDARIES OF CONSUMER MANIPULATION VIA OBA	145
6.1. The EU Legal Framework for OBA	146
6.1.1. EU Consumer Protection Law	146
6.1.2. EU Personal Data Protection Law	152
6.1.3. EU Competition Law	156
6.1.4. EU Digital Single Market	161
6.1.4.1 Before the DSA and the DMA	161
6.1.4.2 The DSA and the DMA	163
6.1.4.3 Artificial Intelligence Act (AIA)	167
6.2. Prohibited OBA Practices	169
6.2.1. The Prohibition of OBA Using Special Categories of Data	170
6.2.2. The Prohibition of OBA for Minors	175
6.2.3. The Prohibition of Profiling with Significant Effects	177
6.2.4. The Prohibition of Unfair Practices and OBA	179
6.2.5. The Proposed Prohibitions of Manipulation via AI	185
6.3. Legal Grounds for OBA	188
6.3.1. Consent	188
6.3.1.1 Conditions	189

6.3.1.2 Consent in AdTech.....	193
6.3.1.3 OBA Contracts	196
6.3.2. Contractual Necessity.....	198
6.3.3. Legitimate Interest	200
6.4. OBA Transparency & Fairness	203
6.4.1. Information Disclosure.....	203
6.4.2. OBA Scrutiny: Archives, Access, Audit.....	206
6.4.3. Managing OBA Risks	209
6.5. Conclusion: Boundaries of Consumer Manipulation via OBA.....	213
CHAPTER 7. CONCLUSIONS: THE ENDS OF OBA.....	216
7.1. Conclusion.....	216
7.2. Recommendations	221
7.3. Going Forward	225
EPILOGUE	228
ACKNOWLEDGMENTS	229
BIBLIOGRAPHY.....	231
GLOSSARY	267
SAMENVATTING (DUTCH SUMMARY).....	270
CURRICULUM VITAE.....	274
INDEX	276

LIST OF FIGURES

Figure 2:1. <i>Real Time Bidding (RTB)</i> (by Veale & Zuiderveen Borgesius).....	33
Figure 3:1. <i>Quadrant of influence with examples</i> (by author)	46
Figure 3:2. <i>Levels of vulnerability</i> (by author).....	65
Figure 3:3. <i>Spectrum of influences with situations</i> (by author).....	66
Figure 4:2. <i>Levels of online consumer vulnerability</i> (by author)	78

LIST OF TABLES

Table 4-1. <i>Manipulative practices for attracting consumers</i> (by author)	84
Table 4-2. <i>Manipulative practices for maximizing engagement</i> (by author)....	87
Table 4-3. <i>Exploitative patterns in cookie banners</i> (by author).....	90
Table 4-4. <i>Manipulative practices for data extraction</i> (by author)	92
Table 4-5. <i>Covert advertising personalization</i> (by author)	97
Table 4-6. <i>Hardship targeting</i> (from Google Ad Policy).....	99
Table 4-7. <i>Targeting identity</i> (from Google Ad Policy, examples added)	100
Table 4-8. <i>Advertising practices that exploit vulnerabilities</i> (by author).....	102
Table 4-9. <i>Manipulative practices of OBA</i> (by author).....	103
Table 5-1. <i>Consumer manipulation harms of OBA</i>	143
Table 6-1. <i>Article 5(1)(a)-(b) EC.AIA, EP.AIA and C.AIA</i> (by author)	185
Table 6-2. <i>The EU Legal framework for consumer manipulation via OBA</i> ...	213
Table 7-1. <i>Safeguarding consumer manipulation harms of OBA</i> (by author)	220

ACRONYMS

AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AVMSD	Audiovisual Media Services Directive
CA	Competition Authority
CFREU	Charter for the Fundamental Rights of the EU
CJEU	The Court of Justice of the European Union
CMP	Consent Management Platform
CRD	Consumer Rights Directive
CPA	Consumer Protection Authority
C.AIA	Council Mandate of AIA
DMA	Digital Markets Act
DPA	Data Protection Authority
DSA	Digital Services Act
DSC	Digital Service Coordinator
DSP	Demand Side Platform
DPIA	Data Protection Impact Assessment
EAIB	European Artificial Intelligence Board
EBDS	European Board for Digital Services
EC	European Commission
ECHR	European Convention of Human Rights
EC.AIA	European Commission Proposal for AIA
ECtHR	The European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EP.AIA	European Parliament Mandate for AIA
EU	European Union
GDN	Google Display Network (GDN)
GDPR	General Data Protection Regulation
OBA	Online Behavioral Advertising
PKM	Persuasion Knowledge Model
RTB	Real-Time Bidding
SSP	Supply Side Platform
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union
UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contract Terms Directive
UK	United Kingdom
US	United States of America
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine

CHAPTER 1. INTRODUCTION: POWER & DIGNITY

1.1. Setting the Stage¹

The rise of digital platform providers as powerful market actors has been one of the defining characteristics of the twenty-first century.² These platforms include search engines,³ social networks,⁴ marketplaces,⁵ app stores,⁶ messengers,⁷ on-demand,⁸ and video-sharing services.⁹ The companies providing these services, such as Alphabet,¹⁰ Amazon, and Meta,¹¹ were nearly bankrupt or non-existent in the early 2000s.¹² In 2022, these three companies exceeded \$4 trillion in market capitalization and joined Apple and Microsoft on the list of the world's most profitable companies, commonly known as Big Tech.¹³ The rise of these companies

¹ Parts of this section were published as the co-authored paper: *See generally*, Lex Zard & Alan M. Sears, *Targeted Advertising and Consumer Protection Law in the European Union*, 56 VAND. J. TRANSNAT'L. L. 799 (2023).

² A digital platform (or platform) is defined in this thesis as a digital service that “facilitates interactions between two or more distinct but independent sets of users (whether firms or individuals) who interact through the service via the Internet.” *See* ORG. FOR ECON. COOP. & DEV., AN INTRODUCTION TO ONLINE PLATFORMS AND THEIR ROLE IN THE DIGITAL TRANSFORMATION, 20 (2019), <http://doi.org/10.1787/53e5f593-en>. The Digital Services Act that regulates digital services in the EU distinguishes between “online platforms” and “online search engines”. *See* Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277), art. 3 (i)-(j) [hereinafter Digital Services Act]. Platform in this thesis has a broader meaning and covers both “online platforms” and “online search engines”.

³ For example, Google Search, Microsoft Bing.

⁴ For example, Facebook, Instagram, Twitter.

⁵ For example, Amazon Store, Google Shopping.

⁶ For example, Google Play, Apple AppStore.

⁷ For example, WhatsApp, Signal.

⁸ For example, Netflix, Amazon Prime.

⁹ For example, YouTube, TikTok.

¹⁰ Alphabet, Inc. [hereinafter Alphabet] is a technology conglomerate that was previously listed on stock market as Google, Inc. Google LLC is now one of the wholly owned subsidiaries of Alphabet and it operates, among other things, Google Search, Google Shopping, Google Play, YouTube, Google Chrome, Android, and Google Maps. *See G is for Google*, ALPHABET, <https://abc.xyz/> (last visited Oct 10, 2022).

¹¹ Meta Inc. [hereinafter Meta] was formerly listed on the stock market as Facebook, Inc., which was incorporated in 2004. It operates Facebook, Instagram and WhatsApp. *See Introducing Meta: A Social Technology Company*, META (Oct. 28, 2021), <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> (last visited Jun 8, 2023).

¹² Luigi Zingales & Filippo Maria Lancieri, *Stigler Committee Digital Platforms: Policy Brief*, 2–6 (2019).

¹³ “Big Tech” refers to five companies: Alphabet, Amazon, Apple, Microsoft, and Meta. In 2021, these companies alongside Saudi Aramco were the largest companies by market capitalization. *See* Jenna Ross, *The Biggest Companies in the World in 2021*, VISUAL CAPITALIST (Jun. 10, 2021), <https://ourworldindata.org/explorers/population-and-demography> (last visited Oct 10, 2022). Since then Meta has dropped on 9th and then 13th place. *See Largest Companies by Market Cap*, COMPANIESMARKETCAP, <https://companiesmarketcap.com/> (last visited Nov 16, 2023). The main source

is unsurprising: their platforms act as the “gateways”¹⁴ to the Internet, where humans spend a large portion of their daily time.¹⁵

In principle, their gatekeeping position allows platform providers to sort consumers into categories and give business users access to these categories.¹⁶ Therefore, platform providers monetize their position as intermediaries by charging business users for consumer attention instead of directly charging consumers a monetary fee.¹⁷ Marketplaces and app stores are *commission-based* platforms: they charge a commission to retailers (or developers) who sell their products (services, content) to the platform consumers.¹⁸

Search engines, social networks, and video-sharing services are primarily *advertising-based* platforms: they charge advertisers for showing their advertisements to platform consumers.¹⁹ The providers of advertising-based platforms have been particularly impactful in shaping the human experience online.²⁰ These companies, notably Alphabet and Meta,²¹ have molded their shared

of revenue for Alphabet, Amazon, and Meta is derived from the monetization of their platforms. While Apple and Microsoft also monetize platforms (e.g., Apple App Store, Microsoft Bing), the majority of their profits come from the sale of computer devices and associated software.

¹⁴ See generally, Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J. L. & TECH. 253 (2006). In the EU, the Digital Markets Act introduced the rules for designating “gatekeepers”. See Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) O.J. 2022 (L 265)1 [hereinafter Digital Markets Act].

¹⁵ Julie E. Cohen, *Law for the Platform Economy*, 51 U. C. DAVIS L. REV. 133, 143 (2017). (“Platforms represent infrastructure-based strategies for introducing friction into networks. In theory, the twenty-first century communications infrastructure still known as the Internet is “open,” and for some purposes, that characterization is accurate. For most practical purposes, however, the “network of networks” is becoming a network of platforms; Internet access and use are intermediated from beginning to end.”)

¹⁶ See *Id.* at 145–148.

¹⁷ See generally, TIM WU, *THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS* (2016). This thesis refers to individual recipients of platform service as consumers. See also Jake Goldenfein & Lee McGuigan, *Managed Sovereigns: How Inconsistent Accounts of the Human Rationalize Platform Advertising*, 3 J. L. & POL. ECON. 425 (2023).

¹⁸ See How to Sell on Amazon, AMAZON, <https://sell.amazon.com/sell> (last visited Nov 15, 2022). See Apple Media Services Terms and Conditions, APPLE LEGAL, <https://www.apple.com/legal/internet-services/itunes/us/terms.html> (last visited Nov 15, 2022).

¹⁹ See How We Make Money with Advertising, GOOGLE, <https://howwemakemoney.withgoogle.com> (last visited Nov 15, 2022). See Terms of Service, FACEBOOK, <https://www.facebook.com/terms.php> (last visited Nov 15, 2022).

²⁰ See SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 63–97 (2019).

²¹ Amazon, Microsoft, and Apple are increasingly involved in monetizing their position for advertising purposes. Amazon, in particular, has become the third gatekeeper with a significant share in online advertising markets. See e.g., Share of ad-selling companies in digital advertising revenue in the United States from 2020 to 2025, STATISTA (2023), <https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/> (last visited Jun 9, 2023). Unlike Alphabet and Meta, online advertising is only a complementary source of revenue for other Big Tech platform providers.

monetization model into the infrastructure that facilitates the “free Internet,” where consumers access most websites and apps without monetary payment.²²

This infrastructure works the following way: platforms provide advertising dashboards, such as Google Ads or Meta Ads Manager, where advertisers choose categories of consumers they want to target with advertising campaigns.²³ These dashboards typically enable targeting consumers categorized based on their search keywords, demographics, and interests, the latter being particularly popular amongst advertisers.²⁴ This feature, also known as online behavioral advertising (OBA), enables advertisers to target consumer segments categorized based on the interests that platforms inferred by analyzing consumer behavioral data.²⁵ For example, the platform’s algorithm may categorize a consumer as a surf enthusiast because they have watched surfing videos. Instead of directly surveying consumers, platforms assume they can accurately predict their genuine interests through algorithmic processes.²⁶

This thesis refers to providers of all digital services, including platforms, that publish advertising on their websites and apps as “publishers” (GLOSSARY).²⁷ OBA requires publishers to maximize consumer behavioral data for optimizing their algorithms’ performance and, thus, revenue.²⁸ Platform providers lead the OBA industry with access to the most consumer behavioral data and the best computation capabilities among publishers. With this imperative, platform providers (e.g., Alphabet and Meta) contract other publishers (e.g., newspapers and gaming) that provide websites and apps over the Internet to join their advertising networks, such as Google Display Network and Meta Audience Network.²⁹ In exchange, platform providers track consumers across the publishers’ websites and apps, optimize their OBA algorithms, and offer advertisers to serve campaigns across the ad network.³⁰

Publishers can also rent their advertising space outside large platforms’ ad networks either privately (providing their own dashboards, e.g., the New York

²² See Julie E. Cohen, *Infrastructuring the Digital Public Sphere*, 25 YALE J. L. & TECH. 1 (2023).

²³ See *Id.*, at 14-28.

²⁴ See e.g., *Explore Advanced Advertising Strategies*, GOOGLE ADS, https://ads.google.com/intl/en_ie/home/resources/advanced/ (last visited Jun 9, 2023).

²⁵ See FREDERIK J. ZUIDERVEEN BORGESIOUS, *IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIORAL TARGETING* 14 (2015). See *About Audience Targeting*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/2497941?hl=en> (last visited Jan 3, 2023).

²⁶ See ZUIDERVEEN BORGESIOUS, *supra* note 25, at 1–2.

²⁷ See *Glossary of Terminology*, IAB, <https://www.iab.com/insights/glossary-of-terminology/> (last visited Jan 3, 2023).

²⁸ See ZUBOFF, *supra* note 20, at 93–98. See JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 3 (2019).

²⁹ See e.g., *Meta Audience Network*, META, <https://www.facebook.com/audiencenetwork/> (last visited Jun 9, 2023).

³⁰ See ZUBOFF, *supra* note 20, at 93–98.

Times) or in the open advertising exchange, sometimes called “AdTech”. Nevertheless, within AdTech, Alphabet provides the largest advertising exchange, Google AdX, that enables all publishers, including platforms and their ad networks, to compete in a fully automated auction process, determining what advertisement is placed on what website or app over the Internet.³¹ In essence, Alphabet provides the largest advertising intermediary in all functions of AdTech. Therefore, through ad networks and ad exchanges, the largest platform providers, such as Alphabet and Meta, provide OBA infrastructure that enables consumers to access most of the Internet without paying a monetary fee.³²

While publishers could execute other forms of (e.g. contextual) advertising, executing OBA privately is challenging as they cannot access necessary data without joining advertising networks or open exchanges. As a response, A myriad of digital service providers have emerged to facilitate the OBA infrastructure. Nevertheless, the largest platform providers that channel most of the consumer attention online have access to unmatched amounts of behavioral data and continue to dominate the advertising markets emerging from the OBA infrastructures.³³ These platform providers collect revenue far exceeding estimated fair returns to their shareholders.³⁴ Studies report that while the OBA infrastructures benefit the large platforms with data advantage (“data power”),³⁵ notably Alphabet and Meta, they do not similarly benefit advertisers, publishers, and consumers dependent on their platforms.³⁶

³¹ See Michael Veale & Frederik Zuiderveen Borgesius, *AdTech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226–227 (2022).

³² See also Cohen, *supra* note 22 at 14–28. See also Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, J. INFO. TECH. (2015), <https://journals-sagepub-com.ezproxy.leidenuniv.nl/doi/10.1057/jit.2015.5> (last visited Oct 28, 2023).

³³ In 2019, in the UK, £14 billion was spent on online advertising, 80% of which were spent on platforms operated by Alphabet and Meta. See COMPETITION & MKTS. AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING: MARKET STUDY FINAL REPORT 9 (2020) [hereinafter CMA (UK) Study on Online Platforms and Digital Advertising].

³⁴ See *Id.*, at 33. See COMISIÓN NACIONAL DEL LOS MERCADO Y LA COMPETENCIA, STUDY ON THE COMPETITION CONDITIONS IN THE ONLINE ADVERTISING SECTOR IN SPAIN E/CNMC/002/2019 143-145 (2021) [hereinafter CNMC (Spain) Study on Competition in Online Advertising].

³⁵ See Antonio Davola & Gianclaudio Malgieri, *Data, Power and Competition Law: The (Im)Possible Mission of the DMA?*, in THE ECONOMICS AND REGULATION OF DIGITAL MARKETS (RESEARCH IN LAW AND ECONOMICS, 31) (2023), <https://papers.ssrn.com/abstract=4242574> (last visited Sep 23, 2023).

³⁶ See CMA (UK) Study on Online Platforms and Digital Advertising, *supra* note 33. See CNMC (Spain) Study on Competition in Online Advertising, *supra* note 34. See EUROPEAN PARLIAMENT, POL’Y DEP’T FOR ECON., SCI. & QUALITY OF LIFE POLICIES, ONLINE ADVERTISING: THE IMPACT OF TARGETED ADVERTISING ON ADVERTISERS, MARKET ACCESS AND CONSUMER CHOICE (2021) [hereinafter European Parliament Study Online Advertising & Consumer Choice]. See EUROPEAN PARLIAMENT, POL’Y DEP’T FOR CITIZENS’ RIGHTS & CONST. AFF., REGULATING TARGETED AND BEHAVIOURAL ADVERTISING IN DIGITAL SERVICES: HOW TO ENSURE USERS’ INFORMED CONSENT (2021) [hereinafter European Parliament (EU) Report on Consent in Targeted & Behavioral Advertising]. See EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY,

The central concern is that OBA infrastructure instrumentalizes the consumers by treating them as “mere means” to maximize profits for large platforms at the center of the infrastructure.³⁷ In particular, it is claimed that the relative profitability of OBA infrastructure in comparison to other forms of advertising stems from disregarding consumer autonomy and manipulating consumers by exploiting their vulnerability in decision-making, leading to a variety of adverse effects, such as loss of time, economic and emotional harm, discrimination, oppression, and psychological and physical detriment.³⁸ In extreme cases, consumer manipulation via OBA may lead to fatal outcomes³⁹ and undermine democracy.⁴⁰

The legal framework of the European Union (EU) heavily regulates OBA. Firstly, as OBA is a business-to-consumer commercial practice, consumer protection law requires businesses engaging in OBA to respect consumer autonomy.⁴¹ The Unfair Commercial Practices Directive (UCPD), more specifically, establishes boundaries for consumer exploitation, including through manipulation.⁴² Secondly, to safeguard consumer privacy, the Directive on Privacy and Electronic

STUDY ON THE IMPACT OF RECENT DEVELOPMENTS IN DIGITAL ADVERTISING ON PRIVACY, PUBLISHERS, AND ADVERTISERS (2023) [hereinafter European Commission Study Recent Digital Advertising Developments].

³⁷ See ZUBOFF, *supra* note 20, at 376–382. See COHEN, *supra* note 28, at 95–96.

³⁸ See Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1025-26, 1029-30 (2014). See Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 162, 166 (2019). See Daniel Susser, Beate Roessler & Helen F. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. & TECH. REV. 1, 38 (2019).

³⁹ Algorithms that rely on behavioral personalization (“profiling”) have been blamed for leading to physical and mental health harm for vulnerable consumers, such as minors. One infamous example is of Molly Russell, whose coroner argued that the social network content personalization algorithm (“recommender system”) led the minor to commit suicide. See Angus Crawford & Bethan Bell, *Molly Russell Inquest: Father Makes Social Media Plea*, BBC NEWS, Sep. 30, 2022, <https://www.bbc.com/news/uk-england-london-63073489> (last visited Mar 28, 2023). See Angus Crawford & Tony Smith, *In Her Own Words - Molly Russell’s Secret Twitter Account*, BBC NEWS, Sep. 21, 2022, <https://www.bbc.com/news/uk-62892636> (last visited Mar 28, 2023). See Matija Franklin et al., *The EU’s AI Act Needs to Address Critical Manipulation Methods*, OECD.AI (Mar. 21, 2023), <https://oecd.ai/en/wonk/ai-act-manipulation-methods> (last visited Mar 28, 2023). Recommender systems are often employed to operationalize OBA, and, thus, are covered by these thesis.

⁴⁰ See Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGAN. THEORY 3 (2022).

⁴¹ See Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, 54 COMMON MKT. L. REV. 1427, 1436 (2017). See JAN TRZASKOWSKI, YOUR PRIVACY IS IMPORTANT TO US! - RESTORING HUMAN DIGNITY IN DATA-DRIVEN MARKETING 181–187 (2021). See FEDERICO GALLI, ALGORITHMIC MARKETING AND EU LAW ON UNFAIR COMMERCIAL PRACTICES 264–265 (2022).

⁴² Directive (EC) 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) 2005 O.J. (L 149) 22 [hereinafter Unfair Commercial Practices Directive]. See TRZASKOWSKI, *supra* note 41, at 29–31.

Communications (ePrivacy Directive) regulates the tracking of consumers across the Internet,⁴³ and the landmark General Data Protection Regulation (GDPR) establishes safeguards against the harms of OBA to consumers when these systems process personal data.⁴⁴ The protection of personal data that OBA requires is a fundamental right in the EU legal framework, intending to safeguard human dignity.⁴⁵ Thirdly, consumer autonomy is also an essential objective of the EU competition policy.⁴⁶ The European Commission is actively enforcing competition law in digital markets, and in 2021, it opened formal antitrust investigations of Alphabet and Meta regarding their advertising practices.⁴⁷

The legal framework of the EU also recognizes new forms of societal and macroeconomic threats stemming from the OBA infrastructures that incentivize and enable consumer manipulation. In particular, arguably, OBA infrastructures threaten democracy by facilitating misinformation and polarization, and they favor large platform providers with data power, further inhibiting innovation.⁴⁸ In 2022, the EU introduced the Digital Services Act (DSA) and the Digital Markets Act (DMA), which regulate platform providers, including their advertising practices.⁴⁹

⁴³ Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 O.J. (L 201) 31 [hereinafter ePrivacy Directive]. *See also Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 (Jan. 10, 2017) [hereinafter Proposal for ePrivacy Regulation].

⁴⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119)1 [hereinafter General Data Protection Regulation]. Personal data protection law reform that resulted in the General Data Protection Regulation was largely triggered by the need to respond to emerging OBA business model. *See* European Commission Press Release IP/10/63, The Commission, Europeans' Privacy will be big challenge in next decade, says EU Commissioner (Jan. 28, 2010), https://ec.europa.eu/commission/presscorner/detail/en/IP_10_63 (last visited Nov 16, 2023).

⁴⁵ Consolidated Version of the Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391 [hereinafter CFREU].

⁴⁶ *See* Inge Graef, *Consumer Sovereignty and Competition Law: From Personalization to Diversity*, 58 COMMON MKT. L. REV. 471, 475-476 (2021).

⁴⁷ *See* European Commission Press Release IP/22/1703, The Commission, Antitrust: Commission opens investigation into possible anticompetitive conduct by Google and Meta, in online display advertising (Mar. 11, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1703 (last visited Nov 16, 2022). *See* European Commission Press Release IP/23/3207, European Commission Press Release IP/23/3207, The Commission, Commission sends Statement of Objections to Google (Jun. 14, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207 (last visited Jun 14, 2023).

⁴⁸ *See Ledger of Harms*, CENTER FOR HUMANE TECHNOLOGY, <https://ledger.humanetech.com/> (last visited Nov 18, 2023).

⁴⁹ Digital Services Act, *supra* note 2. Digital Markets Act, *supra* note 12.

The DSA explicitly prohibits some forms of OBA intending to safeguard against societal consumer manipulation harms.⁵⁰ In contrast, the DMA plans to disperse the data power of designated “gatekeepers” or the most prominent platform providers to ensure contestability in digital markets, including in the OBA infrastructure, promote innovation, and safeguard the authentic choice of consumers.⁵¹ Lastly, by 2024, the EU may finalize drafting the Artificial Intelligence Act (AIA) that sets further boundaries for human manipulation via artificial intelligence (AI), also when used for OBA.⁵²

While the legal framework of the EU heavily regulates OBA, the online environment continues to be plagued by manipulative practices designed for operationalizing OBA infrastructure.⁵³ Some commentators explain this by pointing to the substantive insufficiency of the EU legal framework.⁵⁴ Others blame this on the ineffective enforcement of this framework.⁵⁵ Academic literature typically analyzes OBA through the lens of consumer protection, data protection, and competition law in silos.⁵⁶

Lastly, while there is a growing trend in the EU legal academia to break down the silos of these legal domains,⁵⁷ no academic work has yet evaluated the effectiveness of the EU legal framework as a whole from a unified perspective in protecting against consumer manipulation harms of OBA, which remains a central concern.⁵⁸

⁵⁰ Digital Services Act, *supra* note 2, rec. 69.

⁵¹ Digital Markets Act, *supra* note 12, recs. 1-2. The Digital Markets Act mentions consumer “choice” 23 times.

⁵² See *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter AI Act Proposal].

⁵³ See EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, BEHAVIOURAL STUDY ON UNFAIR COMMERCIAL PRACTICES IN THE DIGITAL ENVIRONMENT: DARK PATTERNS AND MANIPULATIVE PERSONALISATION: FINAL REPORT (2022) [hereinafter European Commission Study Dark Patterns & Manipulative Personalization]. See *Manipulative Online Practices*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418 (last visited Mar 2, 2023).

⁵⁴ See e.g., Philipp Hacker, *Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law*, EUR. L. J. 1-34 (2021).

⁵⁵ See e.g., Johnny Ryan, *Don't Be Fooled By Meta's Fine For Data Breaches, Says Johnny Ryan*, THE ECONOMIST, May 24, 2023, <https://www.economist.com/by-invitation/2023/05/24/dont-be-fooled-by-metas-fine-for-data-breaches-says-johnny-ryan> (last visited May 30, 2023).

⁵⁶ See e.g., for consumer protection: Zard and Sears, *supra* note 1; See e.g., for data protection: ZUIDERVEEN BORGESIU, *supra* note 23; See e.g., for competition law: Graef, *supra* note 41.

⁵⁷ See e.g., Christof Koolen, *Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data*, 31 EUR. REV. PRIV. L. 427-468 (2023).

⁵⁸ See Zuboff, *supra* note 40, at 7-10.

1.2. Research Questions

The central research question (RQ) of this thesis is:

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

This RQ is broken down into five sub-questions (SQs) answered in five chapters, Chapter 2 through Chapter 6. The first sub-question (SQ1) focuses on defining and describing OBA, a central practice studied in this thesis:

SQ1: what is online behavioral advertising (OBA)?

By answering SQ1, Chapter 2 defines what OBA is, delineates related terminology, and describes how OBA works, including its actors. The second sub-question (SQ2) focuses on defining manipulation, which in later chapters is analyzed as the likely result of OBA:

SQ2: what is manipulation?

By answering SQ2, Chapter 3 defines manipulation and delineates it from other forms of influence, such as persuasion and coercion. The third sub-question (SQ3) shifts toward the central phenomenon of this thesis and explores the extent to which OBA results in consumer manipulation:

SQ3: what is consumer manipulation via OBA?

By answering SQ3, Chapter 4 analyzes the manipulative practices of OBA. The fourth sub-question (SQ4) addresses the harms of consumer manipulation via OBA, which is the central issue in this thesis:

SQ4: what are the consumer manipulation harms of OBA?

By answering SQ4, Chapter 5 defines the consumer manipulation harms of OBA as the central problem. The fifth and the last sub-question (SQ5) shifts to evaluating the EU legal framework:

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

By answering SQ5, Chapter 6 elaborates on the EU legal framework's boundaries on consumer manipulation via OBA. Chapter 7 combines answers of all five SQs and formulates the answer to the RQ of this thesis.

1.3. Methodology

This thesis aims to evaluate the effectiveness of the EU legal framework in safeguarding against the consumer manipulation harms of OBA. With this aim in mind, this thesis relied on *desk research*, including analysis of (i) legal texts and (ii) case law, (iii) academic literature, and (iii) online sources.

This thesis analyzes EU primary and secondary law with the scope defined in section 1.4. The EU primary law includes the Treaty of the Functioning of the European Union (TFEU),⁵⁹ the Treaty on the European Union (TEU)⁶⁰, and the Charter of the Fundamental Rights of the European Union (CFREU).⁶¹ These treaties are analyzed in two ways. Firstly, this thesis relies on them to identify interests, such as dignity and the free market, that the legal framework intends to protect. Through such analysis, Chapter 5 constructs the theory of harms that later acts as a lens through which the entire legal framework is evaluated. Secondly, primary law is also a subject of such an evaluation. For example, Chapter 5 evaluates the consistency and completeness of theories of harm in the EU Treaties.⁶²

Apart from the treaties, Chapter 6 evaluates the EU secondary law, including consumer protection, privacy and data protection, competition, and digital single market law. This thesis evaluates legislative acts, such as regulations, directives, decisions, recommendations, and opinions, and non-legislative acts, such as delegated acts and implementing acts, in light of the theory of harm developed in Chapter 5. In order to operationalize this evaluation, this thesis first describes and explains the boundaries of this framework for consumer manipulation via OBA (in section 6.1). This thesis relies on various types of interpretation of legal sources, including legal-historical, grammatical, and teleological.⁶³ In essence, Chapter 6 provides a *discourse analysis* of the EU legal framework by evaluating the content of the legislative documents and examining the underlying assumptions and ideologies.

⁵⁹ Consolidated Version of the Treaty on the Functioning of the European Union, June 7, 2016, 2016 O.J. (C 202) 47 [hereinafter TFEU].

⁶⁰ Consolidated Version of the Treaty of the European Union, October 26, 2012 O.J. (C 326) 15 [hereinafter TEU].

⁶¹ CFREU, *supra* note 46, art.8.

⁶² In addition, evaluating effectiveness of the EU legal framework in Chapter 6 also includes an analysis of the primary law.

⁶³ For example, by placing the GDPR in the historical context, the thesis identifies OBA as one of the issues that triggered the reform (legal-historical interpretation); by analyzing recitals, the thesis identifies the goal of the legislator to ensure consumer autonomy in the context of OBA (teleological interpretation), and by limiting interpretation to the wording of GDPR's norms, the thesis identifies how the industry has interpreted them in a way that misaligns with the legislator's goals (grammatical interpretation).

This thesis relies on the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (hereafter ECtHR).⁶⁴ This thesis relies on ECtHR cases primarily for building a theory of harm in Chapter 5. The CJEU cases are considered in establishing the boundaries of the EU legal framework. The case law of the Member States is also used, as it often precedes cases addressed by the CJEU and, at times, influences EU policy. The case law was primarily identified through academic literature.

The legal sources and case law were, in all cases, accessed via the Internet. In most cases, the research relied on Google Search to find the latest version of the documents in the official databases.⁶⁵ The research accessed primary and secondary law on the official EU law (EUR-lex)⁶⁶ website and the case law on the CJEU (CURIA)⁶⁷ and the ECtHR (HUDOC)⁶⁸ websites. Lastly, the research relied on the professional networks on X (previously Twitter) and LinkedIn to follow the latest developments concerning legislative proposals, such as in the case of the DSA, the DMA, and the AIA, as well as court judgments or other binding decisions, such as decisions of the European Data Protection Board (EDPB).⁶⁹ The final date until the legal sources and case law were considered was 30 October 2023.

This research also relies on a rigorous literature desk review. Fulfilling the primary objective to evaluate how the EU legal framework safeguards against consumer manipulation harms of OBA required this thesis to define and describe OBA (SQ1, Chapter 2), to define manipulation (SQ2, Chapter 3), to explain how OBA can lead to manipulation (SQ3, Chapter 4) and what harms such manipulation result in (SQ4, Chapter 5).⁷⁰ For each of these chapters, most literature was accessed online and was searched on Leiden University Catalogue and, to some extent, Google Search. The literature was selected based on its source, range, and focus. Regarding sources, the thesis prioritizes the official documents of the EU institutions, such as guidelines, studies, opinions, and other reports. Regarding breadth of range, this thesis selected the literature that covered the most research

⁶⁴ See Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 [hereinafter ECHR].

⁶⁵ For legislation, keywords used for search typically included “final text” and the name of the legal document, e.g., “Digital Services Act”. Case law keywords included case numbers, e.g., “C-646/22-1”.

⁶⁶ See *EUR-Lex*, EUROPEAN UNION, <https://eur-lex.europa.eu/homepage.html> (last visited Nov 29, 2022).

⁶⁷ See *CURIA*, EUROPEAN COURT OF JUSTICE, <https://curia.europa.eu/> (last visited Nov 29, 2022).

⁶⁸ See *HUDOC*, EUROPEAN COURT OF HUMAN RIGHTS, <https://hudoc.echr.coe.int> (last visited Nov 29, 2022).

⁶⁹ Particularly useful has been a X account of journalist Luca Bertuzzi: @BertuzLuca, and a LinkedIn account of data protection expert Luis Alberto Montezuma: @luisalbertomontezuma.

⁷⁰ The literature review also supplemented the analysis of the legal sources and the case law in Chapter 6.

questions.⁷¹ Priority was given to literature that addressed topics within the scope of several SQs of this thesis.

Chapter 2 describes and explains how OBA works. Firstly, the Catalogue was searched with the keyword “online behavioral advertising”, and literature was selected based on the most recent publications with the title containing the keyword, prioritizing sources in the following order: papers including literature review, reports of the EU institutions, scholarly books, academic papers, news. These works provided an understanding of OBA across disciplines. Secondly, the Catalogue was searched with the following OBA-related keywords: “online advertising”, “targeted advertising”, “behavioral targeting”, “profiling”, “real-time bidding,” and “cookies”. Literature was selected in the same order as was done for “OBA”.

This thesis adopted an integrative framework for evaluating OBA that included analyzing findings in the literature from the fields of marketing, psychology, sociology, statistics, policy, and law, depending on the aspects of OBA that the section addressed. For example, section 2.3 describes OBA markets and, therefore, primarily relies on statistics and market studies conducted by competition authorities. Generally, priority was given to the most recent publications. Publications before 2000 are considered only when the section addresses historical context. For instance, section 2.1 explains OBA in a historical context and considers the literature published in the 1900s that explains the evolution of advertising. Google Search was used to capture news sources related to OBA.

Chapter 3 and 4 build a theory of consumer manipulation via OBA. Such a theory is built by evaluating philosophical literature, in particular ethics. Firstly, the Catalogue was searched with the keywords “manipulation”, “autonomy”, and “vulnerability”. Edited books combining various perspectives about manipulation and vulnerability were selected to understand a broad range of meanings and functions of these concepts. In a sense, the purpose of Chapter 3 is to inform legal discussions regarding the uses of these terms. Therefore, policymakers and law enforcers must make the theory-building exercise legible and usable. With this in mind, Chapter 3 selects conceptions of manipulation and vulnerability that can be useful for understanding consumer manipulation via OBA and its harms. Therefore, the Catalogue was further searched with keywords such as “online manipulation” and “digital market manipulation”. The literature was analyzed critically: while some arguments are endorsed, some are criticized and abandoned, and a newer theory of consumer manipulation has been developed.

Further, drafts of these chapters were shared with several philosophers whose work this theory of manipulation builds upon. Their feedback was received via

⁷¹ For example, Calo not only addresses manipulation, but also manipulation in digital markets, and harms of such digital market manipulation, providing discourse relevant to SQ2, SQ3, SQ4. *See* Calo, *supra* note 38.

informal interviews and has shaped the theory. Additionally, active participation in conferences and workshops has shaped the final version of the thesis.

This thesis also relied on the professional networks of X and LinkedIn⁷² to stay updated about new publications and pre-prints about related topics. These networks were used to stay up to date about technology trends. These professional networks were the primary way to find journalistic and other non-scientific sources. For journalistic texts, priority has been given to global, market-oriented, or technology-focused journalism, for example, published in the Economist or Wired, but also to news agencies that follow developments in the EU policy, e.g., EurActiv.⁷³

1.4. Scope

This section clarifies the focus of this thesis and explains the scope. The negative impact of OBA historically is formulated in terms of “privacy” harms. This thesis aims to broaden the analysis. OBA threatens privacy by often accessing information about people and sharing it with others without their knowledge. The OBA industry engages in such intrusions of privacy ultimately to maximize profit, the effect of which is claimed to be consumer manipulation as some OBA practices exploit consumers' vulnerabilities. Consumer manipulation and its harms have been particularly challenging to define.⁷⁴ With this in mind, this thesis focuses on developing a comprehensive theory of manipulation via OBA that can contribute towards understanding and safeguarding against its harms.

Typically, literature refers to Internet “users” or “data subjects” whose data the OBA industry processes. Nevertheless, in most cases, people accessing the Internet, including when using search engines or social networks, are in a commercial relationship with these digital service providers and act as “consumers”.⁷⁵ Overlooking this aspect has previously led to hesitation to apply consumer protection rules to the practices. Therefore, this thesis analyzes OBA in a commercial context and refers to the individual recipients of OBA as a “consumer”.

OBA can also be used in a political context. The Cambridge Analytica scandal revealing the manipulative capabilities of OBA took place in the political context.⁷⁶ Such political OBA is associated with its share of potentially adverse effects on elections, political processes, and democratic institutions. Considering these harms, the European Commission has proposed a Regulation on Transparency and

⁷² LinkedIn page of Luis Alberto Montezuma was particularly important source for finding most up to date material.

⁷³ Reporter Luca Bertuzzi was an important news source for this thesis.

⁷⁴ See generally MANIPULATION: THEORY AND PRACTICE (Christian Coons & Michael Weber eds., 2014). See Susser, Roessler, and Nissenbaum, *supra* note 38. See generally THE PHILOSOPHY OF ONLINE MANIPULATION (Fleur Jongepier & Michael Klenk eds., 2022).

⁷⁵ See Goldenfein and McGuigan, *supra* note 17.

⁷⁶ Cambridge Analytica, a political consulting firm, had used Facebook's advertising platform to influence 2016 elections. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 9–12.

Targeting of Political Advertising.⁷⁷ However, the harms of political OBA largely stem from the affordances of the OBA infrastructure in a commercial context.⁷⁸ Therefore, this thesis analyzes *consumer* manipulation, not *citizen* manipulation. Nevertheless, the severity of political OBA harms needs further research.⁷⁹

This thesis does not analyse areas of law that primarily regulate advertising content, such as intellectual property, including copyright and trademarks, that typically safeguard business interests instead of consumer autonomy. This thesis also does not comprehensively analyse the law on non-discrimination and the environment.⁸⁰ Such a scope is justified due to the focus of this thesis on consumer manipulation and consumer autonomy. Nevertheless, analyses of legislation excluded from the scope of this thesis can complement analysis in this thesis, as non-discrimination, environmental, and media pluralism laws are best placed to safeguard against affinity and environmental harms, as well as threats to democracy rising by challenging media pluralism.

1.5. Structure

This thesis is structured as follows:

Chapter 1 sets the stage for this thesis by elaborating on how OBA acts as the infrastructure that enables the monetization of digital services and content online. It focuses on the potential of OBA to manipulate consumers and explains how the EU legal framework limits this practice. This chapter further introduces the research questions, elaborates on the research methods, scopes the research, and illustrates the structure of the thesis.

Chapter 2 answers SQ1 of this thesis and describes what OBA is. Initially, this chapter provides a working definition of OBA and its components. Next, Chapter 2 analyzes OBA from four perspectives. Firstly, it describes OBA as an advertising paradigm that targets consumers based on their observed behavior instead of voluntary disclosure of preferences. Secondly, it describes OBA as one of several

⁷⁷ See *Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising*, COM (2021) 731 final (Nov.25, 2021). [hereinafter *Proposal for Political Advertising Regulation*].

⁷⁸ See ZUBOFF, *supra* note 35, at 27-63.

⁷⁹ See EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 2/2022 On the Proposal for Regulating on the Transparency and Targeting of Political Advertising* (2022).

⁸⁰ See for non-discrimination law: Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*, 35 BERKELEY TECH. L. J. 367 (2020). See also Amit Datta et al., *Discrimination in Online Advertising: A Multidisciplinary Inquiry*, in PROCEEDINGS OF THE 1ST CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY 20 (2018), <https://proceedings.mlr.press/v81/datta18a.html> (last visited Jan 24, 2023). See EUROPEAN DIGITAL RIGHTS (EDRI), *How Online Ads Discriminate: Unequal Harms of Online Advertising in Europe*, <https://edri.org/our-work/how-online-ads-discriminate/>. See Ana Maria Corrêa, *Regulating Targeted Advertising: Addressing Discrimination with Transparency, Fairness, and Auditing Tests Remedies*, 46 COMPUT. L. & SEC. REV. 1, 1-2 (2022). See Alan M. Sears, *The Limits of Online Price Discrimination in Europe*, 21 SCI. TECHNOL. LAW REV. 1, 38-40 (2021).

configurations of online advertising that algorithmically infers consumer interests and traits based on their behavioral data. Thirdly, Chapter 2 describes markets that emerge for facilitating OBA across the Internet. Fourthly, chapter 2 explains the technical infrastructures that support OBA markets, such as tracking technologies and the programmatic auction processes. Lastly, Chapter 2 formulates the answer to SQ1 by highlighting the essence of this practice at the intersections of different perspectives.

Chapter 3 answers SQ2 of this thesis and builds a theory of manipulation. Firstly, Chapter 3 positions manipulation as a form of influence, distinguishes it from other forms such as persuasion and coercion and defines manipulation as a hidden, successful, and intentional influence. Chapter 3 clarifies that manipulation as a hidden influence involves the exploitation of decision-making vulnerabilities. Secondly, Chapter 3 defines decision-making vulnerabilities, such as cognitive biases, desires, emotions, and beliefs. Thirdly, Chapter 3 uses the layered concept of vulnerability to define different levels of manipulateness. Chapter 3 then explains the difference between labeled and layered conceptions of vulnerability, adopts layered conceptions, and illustrates the variety of vulnerability layers that may come from different sources. Finally, chapter 3 formulates an answer to SQ2 by defining manipulation and manipulative practices and proposing a method for evaluating the manipulateness of commercial practices.

Chapter 4 answers SQ3 of this thesis and builds a theory of consumer manipulation via OBA. Chapter 4 starts by placing manipulation in the context of business-to-consumer relationships (“consumer manipulation”). Chapter 4 identifies two sets of manipulative practices in the context of OBA. Firstly, it lists and describes manipulative practices of OBA used to extract consumers’ attention, time, and data. Secondly, it describes manipulative practices of OBA used in the delivery of advertisements. In conclusion, Chapter 4 formulates an answer to SQ3 and provides Table 4-9 with identified manipulative practices in OBA.

Chapter 5 answers SQ4 of this thesis. It builds the theory of consumer manipulation harms of OBA. It synthesizes market-based (welfarist) perspectives and rights-based (dignitarian) perspectives into a coherent theory by resolving inconsistencies using the normative theory of capabilities approach. Chapter 5 uses such a theoretical framework to analyze consumer manipulation harms of OBA. It concludes by answering SQ4 and identifying seven types of harms, including economic, environmental, affinity, privacy, authenticity, integrity, and dignity harms.

Chapter 6 answers SQ5 of this thesis. Firstly, it elaborates on the EU legal framework for consumer manipulation via OBA, including consumer protection law, data protection and privacy law, competition law, and digital single market law. Secondly, it identifies prohibitions of such a framework that set boundaries for OBA. Thirdly, it elaborates on advertising transparency rules that ensure safeguarding against consumer manipulation harms by making OBA practices transparent. Fourth, it analyzes the conditions under which OBA can be regarded as

legitimate. Lastly, the chapter concludes by answering SQ5 and sketching the legal boundaries of OBA in the EU.

Chapter 7 answers the RQ of this thesis. Firstly, it answers the RQ and substantiates the answer. Secondly, it offers two recommendations: bolder enforcement and clearer guidance. Thirdly, it anticipates central challenges for policymakers and academia.

CHAPTER 2. ONLINE BEHAVIORAL ADVERTISING

This thesis evaluates the ability of the European Union (EU) legal framework to safeguard against consumer manipulation harms of online behavioral advertising (OBA). With this aim in mind, it is essential to explain what OBA is and how it leads to consumer manipulation and subsequent harms. This thesis defines OBA as the online phenomenon where consumers are shown advertisements that are personalized based on their behavioral data.⁸¹ This definition has three cumulative components: (i) the advertisement is targeted to individual consumers, (ii) targeting is based on the consumers' observed behavior, and (iii) consumer behavior is observed *and/or* the consumer is targeted online.⁸² This chapter aims to explain OBA by examining these components. With this in mind, Chapter 2 answers the first sub-question of the thesis:

SQ1: what is online behavioral advertising (OBA)?

Chapter 2 answers *SQ1* in five parts: first, it zooms in on the aforementioned three components of OBA from four different perspectives, and second, it combines these perspectives to describe a holistic picture of OBA. Section 2.1 examines OBA from the perspective of advertising efficiency and describes it as an advertising paradigm that OBA attempts to realize. Section 2.2. examines OBA as a specific configuration of advertising technologies advertisers use for their campaigns. Section 2.3 examines OBA as a market for purchasing online advertisement space, explaining the actors, the ecosystem, and the role of data. Section 2.4 examines the infrastructures that facilitate OBA, such as the programmatic auction, tracking technologies, and emerging alternative methods for advertising personalization. Section 2.5 concludes this chapter and answers *SQ1* by combining four perspectives on OBA described in sections 2.1-2.4.

⁸¹ The definition of OBA in this thesis is based on the definition provided in Sophie C. Boerman, Sanne Kruikemeier & Frederik J. Zuiderveen Borgesius, *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46 J. ADVERT. 363, 364 (2017). Boerman, Kruikemeier, and Zuiderveen Borgesius define OBA as the “practice of monitoring people’s online behavior and using the collected information to show people individually targeted advertisements.” As Varnali later argued, the line between online and offline behavior is blurry. For example, this definition may fail to capture instances when advertising is personalized based on offline consumer behavior (e.g., visiting a particular offline store) that has been recorded via tracking technologies (e.g., using Wi-Fi). Kaan Varnali, *Online Behavioral Advertising: An Integrative Review*, 27 J. MARKETING COMM. 93, 106 (2021). Therefore, the definition in this thesis is slightly adapted to cover such instances.

⁸² Boerman, Kruikemeier, and Zuiderveen Borgesius identify two components: “(1) the monitoring or tracking of consumers’ online behavior and (2) use of the collected data to individually target ads.” Boerman, Kruikemeier, and Zuiderveen Borgesius, *supra* note 82, at 364. The definition of this thesis disentangles the role of the Internet in OBA in a separate component.

2.1. The OBA Paradigm

Three components of the OBA definition reveal three premises that form the OBA paradigm: (i) targeting individual consumers with advertisements is beneficial for advertisers and possibly consumers, (ii) consumers' observed behavior reveals what they react to better than voluntary disclosure (e.g., through surveys), and (iii) the Internet can be used to observe and influence consumer behavior. This section describes the historical processes that led to the emergence of these premises and their collision into a single paradigm. Section 2.1.1 explains how the emergence of cable television fragmented once concentrated mass markets and created a need for advertisers to target narrowly specified audiences. Section 2.1.2 explains the move towards the logic of behaviorism in marketing. Section 2.1.3 illustrates how the Internet catalyzed the logic of targeting and behaviorism into OBA – the most profitable paradigm in the history of advertising.⁸³

2.1.1. Targeting

The rise of advertising came with the mass production of goods in industrialized societies, which created the need for producers to inform mass populations.⁸⁴ Therefore, during almost the entire twentieth century, the primary form of advertising has been mass-market advertising, directing advertisements to the most significant number of consumers possible.⁸⁵ In this period, the legacy (mass) media facilitated mass-market advertising through newspapers and magazines, and later through radio since the 1920s and television since the 1950s.⁸⁶ However, this trend started to shift by the 1970s when the proliferation of channels on *cable* television and new technologies such as CD players and home video recorders fragmented the mass market that was no longer concentrated on a handful of broadcast channels.⁸⁷

Targeting practices in advertising were not new phenomena. Marketers have always targeted their consumers with tailored communications: newspapers and magazines have been creating specialized output tailoring their content, including advertisements to specific audiences (primarily based on class, ethnicity, and gender).⁸⁸ Also, in radio and television, the Nielsen Ranking System provided broad

⁸³ See ZUIDERVEEN BORGESIU, *supra* note 52, at 17.

⁸⁴ See JOSEPH TUROW, BREAKING UP AMERICA: ADVERTISERS AND THE NEW MEDIA WORLD 20–21 (1998). About Industrialization and capitalism: See Herbert Marcuse, *Industrialization and Capitalism*, NEW LEFT REV. 3 (1965).

⁸⁵ See TUROW, *supra* note 85, at 20–21. See also Abigail Bartholomew, *Behaviorism's Impact on Advertising: Then and Now*, 37 THESES C. JOURNALISM & MASS COMM. 1, 8 (2013).

⁸⁶ See COHEN, *supra* note 21, at 38. See TUROW, *supra* note 84, at 4.

⁸⁷ See COHEN, *supra* note 21, at 39. See TUROW, *supra* note 84, at 38.

⁸⁸ See TUROW, *supra* note 84, at 27. See also Advertising the Model T, THE HENRY FORD BLOG (Sep. 9, 2015), <https://www.thehenryford.org/explore/blog/advertising-the-model-t/> (last visited Jan 18, 2023).

demographic information about the viewers (i.e., gender and age group).⁸⁹ However, due to the deep fragmentation of the once concentrated market towards the end of the twentieth century, advertisers started looking for new audiences that they could define in finer detail.⁹⁰ As a result, targeted marketing practices such as direct and database marketing have emerged as primary logic, within which advertisers started compiling increasing amounts of consumer data.⁹¹

2.1.2. Behaviorism

In the search to define consumer audiences in newer, more granular ways, the marketing industry not only collected data through voluntary self-disclosure, such as surveys, but increasingly adopted the observational logic that underpins the branch of psychology called *behaviorism*.⁹² Historically, behaviorism understood a human experience as measurable, observable behavior that can be studied, predicted, and influenced without the subject's awareness.⁹³ Since its development as a scientific theory, behaviorism has been applied in marketing – John B. Watson, a psychologist who conceptualized the term in 1924, became the vice president of one of the largest advertising agencies in the 1930s.⁹⁴ While marketers initially used behaviorism to build brand loyalty and tailor advertising messages, behavioral strategies started to be adopted in targeting practices at the end of the twentieth century.⁹⁵

Supermarkets were pioneers in using behavioral information for their targeting campaigns.⁹⁶ A recent example of a supermarket relying on consumer behavioral data to target the consumer with a marketing communication is when *Target Inc.*, a United States (US) store, made headlines in 2012 for its data-driven targeting practices.⁹⁷ By analyzing the shopping behavior of their consumers who disclosed

⁸⁹ See TUROW, *supra* note 84, at 25.

⁹⁰ See ZUIDERVEEN BORGESIU, *supra* note 52, at 17–18. See COHEN, *supra* note 28, at 39. See also IEN ANG, *DESPERATELY SEEKING THE AUDIENCE* 27–36 (1991).

⁹¹ See TUROW, *supra* note 84, at 55–90. See ZUIDERVEEN BORGESIU, *supra* note 52, at 17–18. See Shelly Rodgers, Hugh Cannon & Jensen Moore, *Segmenting Internet Markets*, in *INTERNET ADVERTISING: THEORY AND RESEARCH* 147, 148 (David W. Schumann & Esther Thorson eds., Mahwah, NJ: Lawrence Erlbaum Associates ed. 2007).

⁹² See ZUBOFF, *supra* note 20, at 371–375.

⁹³ See Rodgers, Cannon, and Moore, *supra* note 91, at 148.

⁹⁴ See Bartholomew, *supra* note 85, 8-11.

⁹⁵ See *Id.*; See also COHEN, *supra* note 28, at 21. See also Adam Arvidsson, *On the “Pre-History of The Panoptic Sort”: Mobility in Market Research*, 1 *SURVEILLANCE SOC’Y* 4 (2003).

⁹⁶ See JOSEPH TUROW, *THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER* (2017).

⁹⁷ See Charles Duhigg, *How Companies Learn Your Secrets*, *THE NEW YORK TIMES*, Feb. 16, 2012, <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (last visited Jan 2, 2023). See also Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, *FORBES*, Feb. 16, 2012, <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (last visited Jan 2, 2023).

that they were pregnant, Target constructed a “pregnancy prediction” score.⁹⁸ When new consumers exhibited similar purchasing behavior, Target automatically predicted that they were pregnant and targeted them with related marketing communications (e.g., sending booklets about diapers to the home addresses of their consumers).⁹⁹ However, the internet, in particular platforms such as search engines, arguably provides the best venue for operationalizing such behavioral targeting on a global scale.

2.1.3. The Internet

The Internet is the global network of computer networks that connect, communicate, and exchange data via technical protocols known as the Internet Protocol Suite or TCP/IP.¹⁰⁰ The Internet became accessible to the general public in 1991, with the launch of the World Wide Web (WWW or the Web) – a tool that allowed the representation of digital content stored on computer networks (e.g., documents, text resources) into websites – a presentable form of digital content that could be accessed by anyone connected to the internet.¹⁰¹ Internet users could access websites via typing their uniquely assigned Uniform Resource Locators (URLs) in the address bar of a web browser (e.g., Mosaic or Netscape Navigator – applications created solely for accessing websites), but also by clicking *hyperlinks* – text on the website that directs the user to another website and its digital content.¹⁰²

Some innovators created websites with the sole purpose of searching for other websites. These so-called “online search engines” provided a list of hyperlinks related to the keyword that the internet user typed in the search bar, and as the number of websites proliferated, they became the primary way the internet users accessed the Web.¹⁰³ For example, Yahoo!, initially called “Jerry and David’s Guide to the World Wide Web”, became the most popular website by the year 2000.¹⁰⁴ Nevertheless, since 2000, Yahoo! started relying on the *PageRank algorithm*, an algorithm of its competitor, Google Search, that accomplished unprecedented relevance and efficiency in delivering search results.¹⁰⁵ Google

⁹⁸ See Duhigg, *supra* note 97. See ZUIDERVEEN BORGESIUS, *supra* note 52, at 44.

⁹⁹ See Duhigg, *supra* note 97.

¹⁰⁰ See Michael Aaron Dennis, *Internet: Description, History, Uses, & Facts*, BRITANNICA, <https://www.britannica.com/technology/Internet> (last visited Jan 17, 2023).

¹⁰¹ *World Wide Web*, WIKIPEDIA (2023), https://en.wikipedia.org/w/index.php?title=World_Wide_Web (last visited Jan 17, 2023).

¹⁰² *Id.*

¹⁰³ See also ZUBOFF, *supra* note 20, at 63–98.

¹⁰⁴ See James Eagle, *Animation: The Most Popular Websites by Web Traffic (1993-2022)*, VISUAL CAPITALIST (Sep. 9, 2022), <https://www.visualcapitalist.com/cp/most-popular-websites-by-web-traffic/> (last visited Jan 17, 2023).

¹⁰⁵ See for Google manifesto Sergey Brin & Lawrence Page, *The Anatomy of a Large Scale Hypertextual Web Search Engine*, 30 COMPUTER NETWORKS & ISDN SYS. 107 (1998).

Search's technological superiority stemmed from adopting behaviorist logic – it observed cues of consumers' online behavior, such as the pattern of searched terms, spelling, punctuation, dwell times, and locations that were ignored by other search engines.¹⁰⁶ It used these cues, sometimes called “data exhaust” or “digital breadcrumbs,” to turn the search engine into a recursive algorithmic system that continuously learned and improved the search results.¹⁰⁷ In other words, Google Search increasingly showed internet users what they were looking for, particularly in contrast with its competitors.

The ban on commercial use of online activities was lifted in 1994, but at that time, internet users were primarily members of a homogenous group of middle-to-upper-income college-educated men, and advertisers were slow to show interest.¹⁰⁸ However, by the 2000s, as a more significant part of human society moved online, search engines became a new venue for marketers to reach audiences that now disclosed their interests by typing keywords into the search engine.¹⁰⁹ For example, Overture, which operated GoTo.com, allowed marketers to bid for their websites to be prioritized in the search results: the highest bidder was listed first, the runner-up was listed second, and so forth.¹¹⁰ In contrast, Google Search faced bankruptcy, as its founders, committed to retaining its technological superiority and high standards of search relevance, refused to rely on advertising.¹¹¹

However, in response to the continuous pressure from investors to find a profitable business model, Google Search adopted several forms of online targeted advertising that were claimed to provide the users with an advertisement that they found relevant that could be demonstrated by increased conversion rates – the rate of the number of times consumers clicked the ads.¹¹² One configuration of advertising on Google Search was OBA that, similar to when improving search results, relied on observing consumer behavior and targeting advertisements based on “digital breadcrumbs” Google Search picked up about the consumers. OBA demonstrated the highest conversion rates compared to other configurations, becoming most

¹⁰⁶ See ZUBOFF, *supra* note 20, at 68.

¹⁰⁷ See *Id.* at 68–69.

¹⁰⁸ See Rodgers, Cannon, and Moore, *supra* note 91, at 151.

¹⁰⁹ See ZUIDERVEEN BORGESIU, *supra* note 23, at 18. See also Susie Chang BA, *Internet Segmentation: State-of-the-Art Marketing Applications*, 2 J. SEGMENTATION MARK. 19 (1998).

¹¹⁰ See Saul Hansell, *Google's Toughest Search Is for a Business Model*, THE NEW YORK TIMES, Apr. 8, 2002, <https://www.nytimes.com/2002/04/08/business/google-s-toughest-search-is-for-a-business-model.html> (last visited Jan 17, 2023).

¹¹¹ See *Id.* The founders of Google Search wrote: “We expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers. This type of bias is very difficult to detect but could still have a significant effect on the market... we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm.” Sergey Brin and Lawrence Page, *supra* note 105, Appendix A.

¹¹² See ZUBOFF, *supra* note 34, at 71–82.

popular amongst advertisers and thus becoming Alphabet’s (previously Google) primary revenue stream. Section 2.2 disambiguates OBA by delineating it from related, similar, and overlapping configurations of online advertising.

2.2. The OBA Configuration

This section examines OBA as the configuration of online advertising dashboards where advertisers choose to target consumers grouped based on the interest inferred by consumers’ behavioral data.¹¹³ Online advertising configurations often overlap, making it confusing for an observer to identify the specific characteristics of OBA. With this in mind, section 2.2.1 delineates OBA from other online advertising configurations. Section 2.2.2 disambiguates OBA by explaining the terms used to describe this configuration.

2.2.1. Online Targeted Advertising

Online targeted advertising refers to an online advertising practice that delivers an advertisement tailored to a particular context or an individual consumer.¹¹⁴ Therefore, two major types of online targeted advertising are contextual and personalized advertising.¹¹⁵ Alphabet did not invent online targeted advertising, but it has provided state-of-the-art practice in all forms since 2003. Therefore, further description of online targeted advertising roughly resembles the terminology of Alphabet with regard to these practices.¹¹⁶

In contextual advertising, advertisers target consumers based on the interaction context.¹¹⁷ This may include the digital content on the publisher’s web page or app that the consumer is accessing, the language content is presented in, the time of the day content is accessed, the general geographic location (e.g., country, state) of the

¹¹³ See ZUIDERVEEN BORGESIU, *supra* note 25, at 14.

¹¹⁴ EUROPEAN COMMISSION, CONSUMERS, HEALTH, AGRICULTURE AND FOOD EXECUTIVE AGENCY, CONSUMER MARKET STUDY ON ONLINE MARKET SEGMENTATION THROUGH PERSONALISED PRICING/OFFERS IN THE EUROPEAN UNION FINAL REPORT 31 (2018) [hereinafter European Commission Study Personalization]. Online targeted advertising is one of several online marketing strategies. Other online marketing strategies include, for example, social media influencer marketing. See THE REGULATION OF SOCIAL MEDIA INFLUENCERS (Catalina Goanta & Sofia Ranchordás eds., 2020). OBA, is a sub-type of online targeted advertising that most of the revenue of online platforms and shapes how these platforms are structured, and provides infrastructure for the entire Web.

¹¹⁵ Online classified advertising is another type of online advertising that is not necessarily *targeted* to a particular individual or through algorithmic analysis of the context. Instead, it resembles classic “classified advertising” found on the designated pages of newspapers listing various sponsored offers open to the readership. Craigslist is the most well-known online classified advertising websites. See *craigslist: Amsterdam*, CRAIGSLIST, <https://amsterdam.craigslist.org> (last visited Jan 11, 2023); See JESSA LINGEL, AN INTERNET FOR THE PEOPLE: THE POLITICS AND PROMISE OF CRAIGSLIST (2020), (last visited Jan 11, 2023).

¹¹⁶ See ZUBOFF, *supra* note 20, at 63–98.

¹¹⁷ See *Contextual Targeting*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/1726458?hl=en> (last visited Jan 2, 2023).

content is accessed from, as well as the weather on that location.¹¹⁸ This contextual information allows advertisers to present ads in the correct language, in the correct market, with the awareness of the elements of the day, and achieve relevance by analyzing the content consumers access instead of analyzing information about the consumers themselves.¹¹⁹ For example, suppose a consumer residing in the Netherlands is reading a blog during a rainy afternoon in English about the benefits of running. In that case, contextual advertising may expose them to advertisements in the English language for waterproof running shoes that can be bought and delivered in the Netherlands.

In contrast to contextual advertising, personalized advertising targets individual consumers based on consumer identity or using the data *about* consumers themselves.¹²⁰ Personalized advertising can be based on data that consumers provide voluntarily. Segmented advertising is a stipulatory term used in the policy documents of the EU institutions to describe personalized advertising that relies on *broad demographic* information that the consumers voluntarily disclose by, for example, signing up for digital services or content.¹²¹ Such information usually includes gender, age, country of residence, and, in some instances, the parental status of the consumer.¹²² For example, to promote its business, an exclusively women’s fitness studio located in Amsterdam may choose to target women in the age group of 18–65 who live in Amsterdam.

Personalized advertising can also rely on more *detailed* demographic information, such as the consumer’s education (e.g., high-school graduate), finances (e.g., household income top 10%), relationship status (e.g., married), employment (e.g., tech industry), or other socio-demographic categories.¹²³ Advertisers can build such a consumer *profile* based on the data voluntarily disclosed by the consumer (i.e., “explicit profile”) or based on the data about consumer behavior that they *observed* (“predictive profile”).¹²⁴ Developing *predictive profiles* by algorithmically

¹¹⁸ See Kaifu Zhang & Zsolt Katona, *Contextual Advertising*, 31 *MARKETING SCI.* 980 (2012).

¹¹⁹ Online contextual advertising, does not necessarily rely on personal data – information about the identified or identifiable individual as defined by the General Data Protection Regulation. Nevertheless, such data may be used for “frequency capping”, a practice that establishes the maximum number of times a single user sees the advertisement. See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 26.

¹²⁰ See *Personalized Advertising*, GOOGLE ADVERTISING POLICIES HELP, <https://support.google.com/adspolicy/answer/143465?hl=en> (last visited Jan 2, 2023).

¹²¹ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 19. See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 26.

¹²² See *About Demographic Targeting*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/2580383> (last visited Jan 2, 2023).

¹²³ See *Id.* See *About Detailed Targeting*, META BUSINESS HELP CENTER, <https://www.facebook.com/business/help/182371508761821> (last visited Jan 2, 2023).

¹²⁴ ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2010 on Online Behavioral Advertising* 7 (2010).

inferring attributes based on the observed online behavioral data about the consumer is commonly called “profiling”.¹²⁵ Advertising configuration that relies on such profiling is called OBA.¹²⁶ Observed online behavioral data about the consumer may include social media data (e.g., posts and likes), search data (e.g., history), web browsing data (e.g., media consumption data), mouse cursor movement, keyboard strokes, and location data.¹²⁷

2.2.2. Profiling: Behavioral Personalization

In OBA, consumers can be profiled beyond demographic traits and may include inferring *psychographic* traits such as affinities, interests, values, and lifestyles.¹²⁸ For example, a consumer can be inferred to be a “surf enthusiast”, a “sci-fi fan”, a “dog lover”, someone who “is about to have a wedding anniversary,” or who “recently moved to Hawaii”.¹²⁹ In OBA, inferences about the consumers’ demographic and psychographic traits are made algorithmically, typically via data mining or artificial intelligence (AI), including machine learning (ML) techniques that recognize patterns and correlations in otherwise raw data.¹³⁰ Further, inferences can be drawn through consumers’ similarity with other consumers – a feat called “lookalike audience” or “similar audience”.¹³¹ The latter practice implies using (sometimes voluntarily disclosed) data from a group of people to predict and infer something about a consumer not explicitly part of that group, as described in Target’s pregnancy prediction case explained in section 2.1.2.¹³²

¹²⁵ See European Commission Study Personalization, *supra* note 114, at 49. See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 19. The General Data Protection Regulation defines “profiling” as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” General Data Protection Regulation, *supra* note 45, at 4(4). See also Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, in PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 17 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

¹²⁶ See ZUIDERVEEN BORGESIU, *supra* note 52, at 15.

¹²⁷ See *Id.* at 35–38.

¹²⁸ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 19. See About Audience Targeting, *supra* note 25.

¹²⁹ See About Demographic Targeting, *supra* note 122.

¹³⁰ See *generally* about data mining: BART CUSTERS, THE POWER OF KNOWLEDGE: ETHICAL, LEGAL AND TECHNOLOGICAL ASPECTS OF DATA MINING AND GROUP PROFILING IN EPIDEMIOLOGY (2004). See *generally* about machine learning: GALLI, *supra* note 41.

¹³¹ See *About Lookalike Audiences*, META BUSINESS HELP CENTER, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited Jan 3, 2023). See *About Similar Segments for Search*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/7151628> (last visited Jan 3, 2023).

¹³² See ZUIDERVEEN BORGESIU, *supra* note 52, at 44.

Profiling can also be used for personalizing any digital content more broadly.¹³³ For example, using behavioral data for personalizing search results by changing their order is often called “personalized ranking” – a practice that almost all websites engage in that allows search (e.g., search engines and online marketplaces).¹³⁴ For example, a consumer searching for “boxing gloves” may be presented with offers from different suppliers, where prominence is given to suppliers from which the consumer has already bought other products. Note that algorithms for personalizing digital content are often called “recommender systems.”

In addition, some websites that use recommender systems for personalizing search results allow advertisers to pay prominence to their products (i.e., “paid ranking”).¹³⁵ This thesis addresses paid ranking as part of OBA to the extent to which behavioral personalization considers consumers’ predictive profiles.¹³⁶ In addition, profiling can be used to personalize prices. Online personalized pricing (alternatively “online price discrimination”) refers to offering different online prices for identical products or services to different consumers.¹³⁷ In one example, Amazon was found to vary prices for video games and Kindle e-books based on consumers’ IP addresses.¹³⁸ In rare cases, online personalized pricing can also be OBA, when an advertiser explicitly sponsors differentiation, for example, for placing an advertisement that offers a discount to a consumer based on their previous buying history.¹³⁹

Profiling, or behavioral personalization, can also be used to optimize content other than advertising and search results. Such behavioral personalization of content is often framed as the core practice of digital service and content providers. For example, Netflix claims to provide “personalized digital content service” – referring to its movie recommendation system, and Facebook defines its primary service as

¹³³ See *Id.*, at 49.

¹³⁴ See European Commission Study Personalization, *supra* note 114 at 41–43. The personalized ranking is sometimes conflated with “price-steering”, that refers to personalization to influence consumers’ willingness to pay the price by placing “more or less expensive products at the top of the list.” See Aniko Hannak et al., *Measuring Price Discrimination and Steering on E-Commerce Web Sites*, in PROCEEDINGS 2014 INTERNET MEASUREMENT CONF. 305, 307 (2014).

¹³⁵ See *Commerce Ranking Disclosure*, FACEBOOK, https://www.facebook.com/legal/commerce_ranking (last visited Jan 3, 2023).

¹³⁶ Overture’s (GoTo.com) paid search described in section 2.1.3 was not online behavioral advertising because it presented search results based on keywords and volume of bids, not behavioral profiles of consumers.

¹³⁷ See Frederik J. Zuiderveen Borgesius & Joost Poort, *Online Price Discrimination and EU Data Privacy Law*, 40 J. CONSUMER POL’Y 347, 348 (2017). See Sears, *supra* note 80, at 3.

¹³⁸ See Sears, *supra* note 80, at 3.

¹³⁹ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 63.

the provision of “personalized experience” – referring to its News Feed.¹⁴⁰ While behavioral personalization of content is not the same as OBA, the latter often involves the former. Sometimes, they are bundled together to justify data collection for advertising personalization.¹⁴¹ Also, content personalization can indirectly increase online behavioral advertising revenue by maximizing user engagement.¹⁴² These practices are further discussed in detail in section 4.2 about manipulative design.

Another form of behaviorally personalized advertising is “re-targeting,” which relies exclusively on consumers’ observed shopping behavior and shows consumers ads for the products and services interest they revealed by, for example, adding them to the shopping cart of the online marketplace.¹⁴³ Re-targeting is particularly noticeable for consumers, as they experience being followed by advertisements across the Internet.¹⁴⁴ For example, a consumer who was considering buying a sports jersey on the website of their favorite football club, but stopped at the checkout, can be offered to buy the jersey when he has moved on from the club’s website and is now reading an online newspaper, or checking their feed on social media. Re-targeting is sometimes dubbed as “creepy marketing” because of the following nature of the advertisement.¹⁴⁵

Finally, online behavioral advertising is rarely applied in isolation. Instead, advertising campaigns often combine segmented, contextual, and behavioral targeting features.¹⁴⁶ Therefore, this thesis refers to OBA as all online advertising practices that rely on online behavioral data for personalization.

2.3. The OBA Markets

This section examines OBA as a phenomenon that gives rise to new digital markets. With this in mind, section 2.3.1 explains who the buyers and sellers of OBA are. Section 2.3.2 zooms in on two different forms of OBA intermediation, and section 2.3.3 explains the role of data and platform power in such markets of OBA intermediation.

¹⁴⁰ See *Netflix Terms of Use*, NETFLIX, <https://help.netflix.com/legal/termsfuse> (last visited Jan 12, 2023). See *Terms of Service*, *supra* note 19.

¹⁴¹ See Zard and Sears, *supra* note 1 at 812–813.

¹⁴² See ZUIDERVEEN BORGESIU, *supra* note 25 at 49.

¹⁴³ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 19.

¹⁴⁴ See *Id.*, at 19–20. ZUIDERVEEN BORGESIU, *supra* note 52 at 48.

¹⁴⁵ See Robert Moore et al., *Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation*, 25 *MARKETING MGMT. J.* 42 (2015).

¹⁴⁶ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 20.

2.3.1. Publishers and Advertisers

In this thesis, “publishers” are referred to as the providers of digital services that publish advertising on their online interface (GLOSSARY). Publishers monetize consumer visits by selling online advertising space called “inventory” to advertisers.¹⁴⁷ Although advertisers include large corporations responsible for most of the online advertisement spending (for example, in 2021, HBO Max spent \$635 million, Disney Plus - \$403 million, and Walmart – \$331 million), it also includes much smaller companies or individuals.¹⁴⁸

Similarly, publishers can be individuals that, for example, run personal blogs, but also large corporations that provide news media (e.g., The New York Times, Le Monde), online stores (e.g., Nike, Zara), online games (e.g., Candy Crush Saga, Pokémon Go), or digital platforms (e.g., Google Search, Facebook, Amazon Store, Apple App Store, Uber).¹⁴⁹ Platform providers are the most prominent publishers, as they generate the most of the traffic online. Taking the United Kingdom (UK) as a comparative example, in 2020, internet users spent fifty percent of their time online using the top ten platform services and thirty-seven percent using the platform services of two companies – Alphabet and Meta.¹⁵⁰

The platform services of Alphabet (e.g., Google Search, Google Maps, YouTube) and Meta (e.g., Facebook, Instagram, WhatsApp) are the most prominent advertising publishers because they reach a massive amount of online consumers who find their services of search and social networking almost essential for accessing social, cultural and commercial connectivity.¹⁵¹

To illustrate, Google Search managed ninety percent of all searches in Europe, and Meta’s platform services handled eighty percent of all social network traffic worldwide.¹⁵² Also, in 2020, Alphabet reached ninety percent of all online consumers in the UK, and Meta reached seventy-five percent.¹⁵³ As consumers spend most of their time online using their services, these platforms act as “gates”

¹⁴⁷ See *Glossary of Terminology*, *supra* note 27.

¹⁴⁸ See *Largest Global Advertisers 2021*, STATISTA, <https://www.statista.com/statistics/286448/largest-global-advertisers/> (last visited Jan 12, 2023). See also CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 61.

¹⁴⁹ European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, 26.

¹⁵⁰ See COMPETITION & MARKETS AUTHORITY, *Online Platforms and Digital Advertising: Market Study Appendix C: Market Outcomes* 11 (2020). Four out of five most visited websites worldwide belong to Alphabet and Meta in 2022. See *Most Visited Websites - Top Websites Ranking for December 2022*, SIMILARWEB, <https://www.similarweb.com/top-websites/> (last visited Jan 12, 2023).

¹⁵¹ See COHEN, *supra* note 28, at 44.

¹⁵² See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 19.

¹⁵³ CMA (UK) Study Online Platforms & Digital Advertising Appendix C, *supra* note 150 at 11.

through which business users can access consumers; therefore, providers of these platforms are sometimes called “gatekeepers”.¹⁵⁴

In exchange for giving the consumers access to their now essential services, gatekeepers assume access to the data about online consumer behavior (i.e., “access-data bargain”), and by applying algorithmic techniques to these data, they render consumers legible.¹⁵⁵ In other words, by analyzing online behavioral data about the individual consumer and consumers in the aggregate, gatekeepers can define narrow consumer segments, profile individual consumers based on their predicted behavior (inferred from their past online behavior), and allocate them into pre-defined or custom segments (e.g., “surf-enthusiast”, “recently divorced”).¹⁵⁶ These capabilities equip gatekeepers to be at the center of OBA intermediation for other publishers and advertisers.

2.3.2. Walled Gardens and AdTech

Non-platform publishers, such as providers of some online newspapers, stores, or games (GLOSSARY), lack capabilities of intermediation and legibility that platforms, especially gatekeepers, wield and cannot build extensive predictive profiles about the consumers. In response to the demand of non-platform publishers to mimic OBA practices, the platform providers have expanded their OBA practices beyond their services by creating advertising networks (“ad networks”), for example, Alphabet’s *Google Display Network* (GDN) and Meta’s Audience Network (AN).¹⁵⁷

These ad networks provide publishers with outsourced sales of advertising space and provide advertisers with aggregated advertising spaces from numerous publishers (GLOSSARY). Ad networks also provide unique targeting capabilities and ad optimization tools. By creating ad networks, platform service providers

¹⁵⁴ See Zittrain, *supra* note 14. See also GIOVANNI DE GREGORIO, DIGITAL CONSTITUTIONALISM IN EUROPE: REFRAMING RIGHTS AND POWERS IN THE ALGORITHMIC SOCIETY 17 (2022). “Very large online platform (VLOP)” has a specific legal meaning in Digital Services Act and, therefore, is addressed in more detail in 6.1.4.2 See Digital Services Act, *supra* note 2. Likewise, “gatekeeper” has a specific legal meaning in Digital Markets Act, and is, therefore, addressed in more detail in 6.1.4.2. See Digital Markets Act, *supra* note 14. On September 6, the European Commission designated six gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft for twenty-two platforms they provide. European Commission Press Release IP/23/4328, The Commission, Digital Markets Act: Commission designates six gatekeepers (Sep. 6, 2023), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328 (last visited Oct 10, 2023).

¹⁵⁵ See COHEN, *supra* note 28 at 37–47.

¹⁵⁶ See *Id.*

¹⁵⁷ See *Glossary of Terminology*, *supra* note 27. Platforms provide self-service interfaces (e.g., Google Ads, Facebook’s Ads Manager) where advertisers select their goals, targeting criteria, and bid amounts or budget. See *Estimate Your Results with Bid, Budget and Target Simulators*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2470105?hl=en&ref_topic=3122864 (last visited Jan 4, 2023).

intermediate between advertisers and other publishers that would not be able to provide similar OBA optimization independently.¹⁵⁸

For example, a large advertiser, such as Nike, wants to advertise its new waterproof running shoes to reach the largest number of online consumers who are enthusiastic about running and live in rainy countries. *Google Ads* uses extensive behavioral data about the consumers to profile them and follow them on the websites of all publishers that joined *GDN*, for example, the online newspaper *The Economist*. By using *Google Ads*, including *GDN*, Nike can target particular consumers on Alphabet’s platform services, such as Google Search, YouTube, but also every other publisher who joined *GDN*.¹⁵⁹ Moreover, by joining *GDN*, *the Economist* can access predictive profiles (e.g., identify visiting consumers as “running enthusiasts”) that they would not be able to generate without joining.

Such ad networks are often called “walled gardens”—closed ecosystems in which platforms provide complete end-to-end intermediation, including technical solutions for advertisers and other publishers.¹⁶⁰ However, in response to the impetus of many publishers and advertisers to escape the complete dependence on platform providers for participating in OBA, new and smaller ad intermediaries have emerged that take on particular functions in the “open exchange” that allow advertisers and publishers to reach consumers over the entire Web.¹⁶¹ Due to the highly technical nature of open exchange advertising, the intermediaries involved, infrastructures, and sometimes the entire open exchange market are called “AdTech”(GLOSSARY).¹⁶²

In AdTech, Demand Side Platforms (DSPs) provide advertisers with a one-stop platform for buying advertising spaces or inventories from many different sources (usually every possible source online).¹⁶³ For example, Nike can use the services of MediaMath (the first DSP launched in 2007) to optimize its advertising expenditure by minimizing waste and placing an advertisement to the consumers for whom the advertisement is maximally relevant.¹⁶⁴ MediaMath aggregates the demand from all its advertising partners and buys advertising spaces in the open exchange according to these demands. In a simplified example, this can be that its two partners, Nike and Adidas, look for inventories (advertising spaces) in the entire internet that enable them to show an advertisement to their preferred audiences. As Nike indicated to

¹⁵⁸ See ZUBOFF, *supra* note 20 at 93–97.

¹⁵⁹ *Google AdSense* includes other websites and apps partnered with Alphabet for online advertising.

¹⁶⁰ CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 155.

¹⁶¹ See *Id.* at 263–265.

¹⁶² See e.g., European Commission Press Release IP/23/3207, The Commission, *supra* note 47.

¹⁶³ See *Glossary of Terminology*, *supra* note 27.

¹⁶⁴ See *MediaMath - Future-Proofed DSP*, MEDIAMATH, <https://www.mediamath.com/> (last visited Jan 18, 2023).

MediaMath that it favors consumers who are “running enthusiasts” that live in rainy countries, it will buy an inventory shown to a consumer that closely resembles Nike’s preferred audience as much as possible. It separately meets Adidas’s demands. As it has detailed insights into what each advertiser is looking for, MediaMath can automate the process to maximize efficiency for all its clients. The upside of using DSPs instead of an end-to-end ad network is that, in looking for advertising spaces, DSP can consider many ad networks that participate in the open exchange, including gatekeepers’ walled gardens and other publishers who do not participate outside of these gardens. The downside is that competition for ad spaces can be more demanding in the open exchange, resulting in difficulty getting the best audiences or higher costs.

Supply-side platforms (SSPs) aggregate publishers’ inventories and sell them in the open exchange.¹⁶⁵ So, for example, if the New York Times (NYT) wants to monetize its online readership, enhance the user experience by providing relevant advertising, and maximize advertising profit, it can use the services of Xandr (one of the SSPs), which aggregates (or packages) inventories of NYT with the inventories of its other clients.¹⁶⁶ When Xandr identifies a particular demand for running enthusiasts who live in the rainy country and that such a consumer visits the NYT, Xander sells the advertising space to the DSP of Nike, which was looking for such a consumer. The exchange of information about the demands and the supply of the available inventory happens on the advertising exchanges (“ad exchange”), which also run the real-time auction process through which inventories are bought and sold.¹⁶⁷ The entire process occurs programmatically (fully automated) and happens almost in the same instance as a consumer visiting a particular website (see the overview of this programmatic process in section 2.4).¹⁶⁸

Many publishers do not have access to consumer behavioral data that is essential to meet the demands of successful behavioral personalization, and many advertisers may not know various new audiences they can reach. Therefore, data management platforms (DMPs) have emerged to support the demand side and supply side by enriching them with data and enabling them to define and target more narrowed-down consumer audiences.¹⁶⁹ Lastly, advertising servers (“ad servers”) provide services to advertisers and publishers for them to track, manage, and measure advertising campaigns.¹⁷⁰ Advertisers’ ad servers offer a centralized tool for managing their campaigns, including uploading advertising designs (i.e.,

¹⁶⁵ See *Glossary of Terminology*, *supra* note 27.

¹⁶⁶ See *Publisher Platforms*, XANDR, <https://www.xandr.com/solutions/monetize/> (last visited Jan 18, 2023).

¹⁶⁷ See *Glossary of Terminology*, *supra* note 27.

¹⁶⁸ See *Id.*

¹⁶⁹ CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 125.

¹⁷⁰ See *Glossary of Terminology*, *supra* note 27.

creative), setting targeting criteria, or measuring performance goals across various DSPs.¹⁷¹ Similarly, publishers' ad servers provide a centralized tool for publishers to optimize monetization from targeted advertising by, for example, managing all of their inventory (websites, mobile apps, videos, games), placing trackers, getting detailed reports, and connecting to multiple SSPs or ad networks.¹⁷²

2.3.3. Markets and Power

Because of the existence of myriads of players within AdTech or the OBA open exchange, its technological and structural complexity has attracted much attention from academia.¹⁷³ Moreover, the industry continuously emphasizes the value that OBA creates for these AdTech participants, placing them at the centre of the discussions around OBA.¹⁷⁴ Nevertheless, only a small piece of OBA revenue is generated in the open exchange. Most of the online advertising revenue is channelled by the most prominent platforms. To illustrate this, in 2021, more than 80% of global online advertising revenue went to platform providers and more than 60% to platforms operated only by Alphabet and Meta.¹⁷⁵ In 2022, more than 50% of online advertising revenue went to Alphabet (\$168.44 billion) and Meta (\$112.68 billion).¹⁷⁶

The competition authorities often differentiate between several online advertising markets, depending on the advertising channels, such as *search* and *display* advertising. Search advertising consists of delivering search ads tailored to the consumer, typically based on search keywords (contextual), but sometimes also based on consumer behavior, qualifying it as a form of OBA in those cases.¹⁷⁷

¹⁷¹ See *Introducing Campaign Manager 360*, CAMPAIGN MANAGER 360 HELP, https://support.google.com/campaignmanager/answer/10157783?hl=en&ref_topic=2758513 (last visited Jan 5, 2023).

¹⁷² See *Advertising with Google Ad Manager*, GOOGLE AD MANAGER HELP, <https://support.google.com/admanager/answer/6022000?hl=en> (last visited Jan 5, 2023).

¹⁷³ See Varnali, *supra* note 81.

¹⁷⁴ *The Value of Digital Advertising*, IAB EUROPE, <https://iabeuropa.eu/the-value-of-digital-advertising/> (last visited Jan 16, 2023).

¹⁷⁵ Alphabet and Meta are often referred to as “duopoly” (or “quasi-duopoly”) in online advertising. See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 39. See European Commission Study Personalization, *supra* note 114, at 41–42. However, Amazon has been rising as an advertising intermediary, and, therefore, triggering new references to “triopoly”. See Google, Facebook, and Amazon: From Duopoly To Triopoly of Advertising, FORBES, Sep. 4, 2019, <https://www.forbes.com/sites/forrester/2019/09/04/google-facebook-and-amazon-from-duopoly-to-triopoly-of-advertising/> (last visited Jan 4, 2023). In the UK, platforms of Google and Meta received 80% of online advertising revenue in 2019. See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 10.

¹⁷⁶ Ronan Shields, *Here Are the 2022 Global Media Rankings by Ad Spend: Google, Facebook Remain Dominant -- Alibaba, ByteDance in the Mix*, DIGIDAY (Dec. 13, 2022), <https://digiday.com/media/the-rundown-here-are-the-2022-global-media-rankings-by-ad-spend-google-facebook-remain-dominant-alibaba-bytedance-in-the-mix/> (last visited Jan 12, 2023).

¹⁷⁷ See European Commission Study Personalization, *supra* note 36, at 16.

Alphabet is by far the single dominant actor in search advertising in the EU.¹⁷⁸ Display advertising consists of delivering banner or video ads (e.g., before the video begins) typically based on consumer behavior, qualifying it often as OBA. The market studies often single out the social media advertising market, as the largest share of display advertising happens on social media platforms (e.g., Facebook, Instagram, and YouTube).¹⁷⁹ Meta dominates the social media advertising market. The rest of the display advertising market, sometimes called the “open display” market, is where all other (non-search, non-social media) publishers, including smaller platforms, compete to sell advertising space. In the UK, the open display market amounts to 15% of total online advertising revenue.¹⁸⁰ In 2019, in Spain, Meta generated more display advertising revenue than all other publishers combined.¹⁸¹ Even in the open display market, platforms wield a significant power. This market is intermediated by the walled gardens of large platforms, such as Alphabet and Meta, as well as AdTech.

Within AdTech, Alphabet provides the largest advertising intermediaries in all functions.¹⁸² Google Marketing Platform combines the most extensive DSP (Display and Video 360) and the most prominent ad server for advertisers (Campaign Manager 360).¹⁸³ Google Ad Manager provides the largest SSP (DoubleClick for Publishers) and the most prominent ad server for publishers.¹⁸⁴ Finally, Google Authorized Buyers or Google AdX is the largest ad exchange.¹⁸⁵ While these intermediaries provide services for publishers and advertisers, they are often found to be self-serving for Alphabet.¹⁸⁶ In other words, AdTech can be seen as another walled garden of Alphabet.

The OBA industry, led by Alphabet and Meta, claims that behavioral personalization is the most efficient configuration (in contrast to contextual or segmented advertising) that creates value for publishers, advertisers, and consumers alike.¹⁸⁷ These claims point towards a higher “click-through rate” or CTR, which

¹⁷⁸ Alphabet held 70% of the search advertising market in France, and 90% in Spain and the UK. *See Id.* at 21.

¹⁷⁹ *See Id.* at 16.

¹⁸⁰ *See* CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 6. *See* European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 38–39.

¹⁸¹ European Commission Study Personalization, *supra* note 36, at 16.

¹⁸² *See* COMPETITION & MARKETS AUTHORITY, *Online Platforms and Digital Advertising: Market Study Appendix M: Intermediation in Open Display Advertising* (2020).

¹⁸³ *See Id.* at 71.

¹⁸⁴ *See Id.* at 12.

¹⁸⁵ CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 12.

¹⁸⁶ *See* European Commission Press Release IP/23/3207, The Commission, *supra* note 47.

¹⁸⁷ Such claims suggest that online behavioral advertising, optimizes advertising expenditure for advertisers and publishers and, on the other hand, provides personalized (and relevant) ads for consumers, as well as funding structure for the entire internet, where consumers can access digital

measures the percentage of consumer action, such as a consumer clicking the ad when exposed to a particular advertisement.¹⁸⁸ For example, one such industry-funded study estimated that the CTR of behavioral personalization is 5 to 10 times higher than other forms of targeting in online advertising.¹⁸⁹ Nevertheless, some evidence shows the contrary.¹⁹⁰ For example, the New York Times, which has cut off OBA open exchange to rely on contextual advertising instead, declared that its revenues have significantly grown.¹⁹¹

These doubts also come with the claim that gatekeepers are the only beneficiaries of OBA markets, as this practice maximizes their profits at the expense of all other participants.¹⁹² For an illustration of platforms' profitability, the UK's Competition and Market Authority has found that Alphabet and Meta had been generating excess profit for their investors (Alphabet returned 40% of capital and Meta 50% to their investors, instead of the expected 8% that would be a fair mark).¹⁹³ In contrast to such an increase in advertising profits for the gatekeepers, the revenue of other players in the industry, publishers, advertisers, and other intermediaries have not significantly changed. Studies attribute this to the gatekeepers' control of internet access and corresponding data that OBA relies.¹⁹⁴

2.4. The OBA Infrastructures

This section describes the infrastructures that facilitate OBA and support the monetization of the Web. Section 2.4.1 describes a programmatic auction process that enables the selection of an advertisement among millions of competitors in milliseconds, section 2.4.2 describes cookies and other tracking technologies that have been used for behavioral personalization, and section 2.4.3 describes alternative models that are emerging due to obvious illegality of historical tracking methods.

content and services they value without monetary payment. *The Value of Digital Advertising*, *supra* note 174. Varnali, *supra* note 81, at 94.

¹⁸⁸See *Clickthrough Rate (CTR): Definition*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2615875?hl=en&ref_topic=24937 (last visited Jan 4, 2023).

¹⁸⁹ *The Value of Digital Advertising*, *supra* note 174.

¹⁹⁰ European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 19–20.

¹⁹¹ See Natasha Lomas, *The Case Against Behavioral Advertising Is Stacking Up*, TECHCRUNCH (Jan. 20, 2019), <https://techcrunch.com/2019/01/20/dont-be-creepy/> (last visited Jan 18, 2023). See Jessica Davies, *After GDPR, The New York Times Cut off Ad Exchanges in Europe -- and Kept Growing Ad Revenue*, DIGIDAY (Jan. 16, 2019), <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/> (last visited Jan 18, 2023).

¹⁹² See Lomas, *supra* note 191.

¹⁹³ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, 8.

¹⁹⁴ European Commission Study Recent Digital Advertising Developments, *supra* note 36, at 16.

2.4.1. Real-Time Bidding (RTB)

In OBA, advertising placements are determined programmatically, that is, by algorithmic systems instead of human-mediated ways.¹⁹⁵ In this programmatic process, advertisers bid on the Real-Time Bidding (RTB) auction to compete with other advertisers to target an ad to a specific consumer online.¹⁹⁶ In the OBA open exchange or AdTech, the RTB auction is housed by the ad exchanges, where SSPs sell the advertising inventory of their publishers and DSPs place bids for their advertisers.¹⁹⁷ The consumer visiting the publisher’s website initiates the programmatic process. Using the trackers placed on the website (section 2.4.2), the publisher’s SSP (or an ad server in case of multiple SSPs) generates an advertisement request (“bid request”) that contains a broad array of information about the consumer seeing the ad inventory.¹⁹⁸

Further, bid requests are passed to ad exchanges and to the DSPs that evaluate advertising opportunities based on their campaign objectives and respond with their bids, the amount of money the advertiser is willing to pay per click.¹⁹⁹ The publishers (via SSP or an ad server) rank the offers based on the price (and other priorities) and decide which advertisement will be served on the webpage (Figure 2:1).²⁰⁰

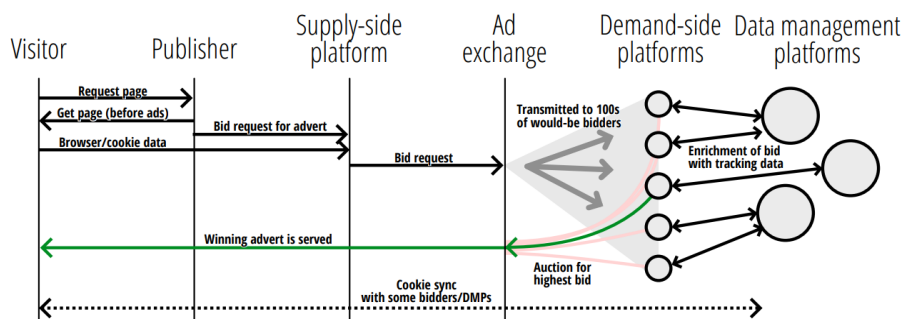


Figure 2:1. Real Time Bidding (RTB) Process (by Veale and Zuiderveen Borgesius)²⁰¹

¹⁹⁵ See Veale and Zuiderveen Borgesius, *supra* note 31 at 231.

¹⁹⁶ *Id.*

¹⁹⁷ European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 25.

¹⁹⁸ See *Authorized Buyers Real-time Bidding Proto*, GOOGLE DEVELOPERS, <https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide> (last visited Jan 5, 2023). See *OpenRTB Integration*, GOOGLE DEVELOPERS, <https://developers.google.com/authorized-buyers/rtb/openrtb-guide> (last visited Jan 5, 2023).

¹⁹⁹ In most cases, advertisers pay per action (“cost-per-action” or CPA), for example, per click on the advertisement (“cost-per-click” or CPC). See *Estimate Your Results with Bid, Budget and Target Simulators*, *supra* note 157. See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33, at 265.

²⁰⁰ CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 265.

²⁰¹ Veale and Zuiderveen Borgesius, *supra* note 31, at 232.

Traditionally, RTB relied on a waterfall auction, in which ad exchanges and SSPs would rank their demand partners sequentially in hierarchical levels (if DSP#1 makes a bid, it gets the inventory; if not, a new auction is triggered for DSP#2, and so forth).²⁰² This enabled large players, such as Alphabet, to prefer their own ad intermediaries that were vertically integrated into the AdTech, and bids would be passed to other DSPs (who may have paid higher prices) only if Alphabet was not interested or did not meet the publisher's requirements.²⁰³ In response to this, the industry developed the *header bidding* protocol that allows queries of the multiple ad exchanges, DSPs, and advertisers simultaneously, and because it allows publishers more freedom to choose whom they sell the advertising space to (prices for which also increased), became the prominent protocol.²⁰⁴

The content of the bid requests is determined by the specifications of *Authorized Buyers* maintained by Alphabet or the *OpenRTB/AdCom* protocol maintained by the Interactive Advertising Bureau (IAB), a membership organization of advertising firms.²⁰⁵ It usually contains information about the consumer, such as age, gender, geographic location (e.g., postal code, longitude, and latitude), metadata about if the consent is provided, or interests, as well as the information about the device that the consumer is using.²⁰⁶ Although the bid requests with some or all of this information give DSPs the possibility to target the consumers in granular ways, the economic incentives of RTB auction mean that DSPs with more specific knowledge about the individual consumers will win the desirable viewers.²⁰⁷ With this in mind, DSPs employ DMPs that help them identify the consumer and enrich the DSP with data about the consumer from other sources (e.g., its database and data brokers).²⁰⁸ A DSP with the most knowledge, wins the auction and links the further data to the consumer for future profiling.

The centrality of the consumer data in the RTB process comes from the advertising paradigm of OBA, which works on the premise that targeting based on consumers' behavioral profiles ensures relevance. With this in mind, the advertisers participating in RTB have an economic incentive to ensure that they bid and compete only in cases where the winning bid maximizes the chance of the consumers clicking the advertisement. Therefore, DSPs and advertising networks

²⁰² See Michalis Pachilakis et al., *No More Chasing Waterfalls: A Measurement Study of the Header Bidding Ad-Ecosystem* (2019) <http://arxiv.org/abs/1907.12649> (last visited Jan 19, 2023).

²⁰³ See Veale and Zuiderveen Borgesius, *supra* note 31, at 32.

²⁰⁴ See Pachilakis et al., *supra* note 201.

²⁰⁵ See *OpenRTB (Real-Time Bidding)*, IAB TECH LAB, <https://iabtechlab.com/standards/openrtb/> (last visited Jan 19, 2023). See *Authorized Buyers Real-time Bidding Proto*, *supra* note 198.

²⁰⁶ See Veale and Zuiderveen Borgesius, *supra* note 31, at 232.

²⁰⁷ *Id.*

²⁰⁸ *Id.*

provide data-based algorithmic tools to estimate CTR into “quality scores”.²⁰⁹ Moreover, such advanced data analytic tools allow advertisers to observe how their advertisements perform (how consumers behave regarding their advertisements) and further tailor their campaigns based on these insights, creating a self-improving optimization cycle.²¹⁰ As the advertisers with more data and more accurate data about the consumer can better estimate such quality scores, the quantity and the quality of data about the consumers and their behavior determines the efficacy of ad optimization.²¹¹

2.4.2. Cookies and Mobile IDs

The most prevalent way to track consumers has been via trackers known as “cookies”.²¹² Cookies are small blocks of encoded or encrypted data that the website’s server places on the consumer’s computer (that visits the website) and later accesses and reads to identify the returning user.²¹³ In the early days of the internet, publishers could not tell the difference between visitors.²¹⁴ Cookies were introduced in 1994 by Netscape Navigator, primarily to “give Web a memory” or, in other words, to identify the re-visiting users on the website.²¹⁵ To illustrate: when the user requests the webpage www.example.com and the request contains no cookies, the server *example.com* presumes this is the first webpage the user visits, so it creates a unique identifier (a string of random numbers and letters) and sends it back to the browser together with the web page.²¹⁶ From this point onwards, whenever the user visits any webpage of *example.com*, the cookie will automatically be sent to the browser. This way, *example.com* has access to the log of information about when the user (singled out with the unique identifier) visited each page.

²⁰⁹ See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36, at 18.

²¹⁰ See ZUBOFF, *supra* note 20, at 93–97.

²¹¹ See *About Quality Score*, GOOGLE ADS HELP, <https://support.google.com/googleads/answer/6167118?hl=en> (last visited Jan 4, 2023). While general criteria of programmatic auctions are known, and analytics tools enable optimizing the campaigns for advertisers, algorithms that underlie these processes are essentially black-box. See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 16.

²¹² See Veale and Zuiderveen Borgesius, *supra* note 31, at 227–229.

²¹³ *Id.* at 227.

²¹⁴ “At that moment in Web history, every visit to a site was like the first, with no automatic way to record that a visitor had dropped by before. Any commercial transaction would have to be handled from start to finish in one visit, and visitors would have to work their way through the same clicks again and again; it was like visiting a store where the shopkeeper had amnesia.” John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, THE NEW YORK TIMES, Sep. 4, 2001, <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> (last visited Jan 5, 2023).

²¹⁵ See ZUIDERVEEN BORGESIOUS, *supra* note 52, at 20.

²¹⁶ *HTTP Cookie*, WIKIPEDIA (2022), https://en.wikipedia.org/w/index.php?title=HTTP_cookie (last visited Jan 19, 2023).

Today, cookies are used for various purposes: they can be *strictly necessary* for enabling website features, for example, accessing secure areas of the website or adding items to a shopping cart.²¹⁷ They can also be used to *improve performance*, such as tracking errors or which website pages are most visited.²¹⁸ They can also enable other *functionalities*, for example, to keep users logged in or retain their preferences.²¹⁹ Such cookies are also called first-party cookies as they are placed by the server of the publisher’s website that the consumer visits (i.e., first-party). There are also *third-party* cookies placed by a party other than the publisher, such as an advertising network.

Initially, placing the third-party cookies was impossible because every web page typically contained digital content only from a single source – the website’s server. However, in 1996, Netscape Navigator 2.0 introduced the so-called “frame” – a function that allowed web page parts to be sourced from other servers.²²⁰ The frame function enabled website publishers to make the digital content of third parties available to consumers. For example, today, the frame function is used to embed a video uploaded on a video-streaming platform such as YouTube on other websites.²²¹ In addition, the “Same Origin Policy” of Navigator 2.0 provided a security protocol to limit the access to cookies to the party that placed them.²²² This entails, for example, that only YouTube’s server accesses the cookies it installed to deliver the video on the publisher’s website.

While third-party cookies can provide significant functionalities (e.g., showing a video from another source), they also allow tracking of the users across the internet and, therefore, have been used to operationalize OBA.²²³ For example, a 2015 study of 478 websites across eight EU member states found that 70% of the 16,555 cookies placed were third-party cookies, from which more than half were set by 25 domains that belonged to advertising intermediaries engaged in OBA.²²⁴ In practice, advertising intermediaries place tracking cookies by placing frames, also

²¹⁷ See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 44.

²¹⁸ *Id.*

²¹⁹ See Katie Moser, *How to Personalize Content Using First Party Cookies and Data*, ZESTY (May 11, 2022), <https://www.zesty.io/mindshare/how-to-personalize-content-using-first-party-cookies-and-data/> (last visited Jan 4, 2023).

²²⁰ See Veale and Zuiderveen Borgesius, *supra* note 31, at 228.

²²¹ See *Embed Videos & Playlists*, YOUTUBE HELP, <https://support.google.com/youtube/answer/171780?hl=en> (last visited Jan 19, 2023).

²²² See Veale and Zuiderveen Borgesius, *supra* note 31, at 4–5.

²²³ See Frederik Braun, *Origin Policy Enforcement in Modern Browsers* (Oct. 26, 2023) (unpublished PhD dissertation, Ruhr Universität Bochum).

²²⁴ See ARTICLE 29 DATA PROTECTION WORKING PARTY, *Cookie Sweep Combined Analyzis - Report*, 14/EN WP 229, 2 (2015).

called “tags” (or “web beacons”), on websites across the internet.²²⁵ These tags can be as big as the advertising box, a space in which an advertisement appears, but as small as a single pixel (“pixel tags” or “1x1 pixels”). For example, tags often take the form of clickable buttons, such as “LOG IN via Facebook” or “SUBSCRIBE to YouTube”.²²⁶

In addition to placing cookies, the tags serve several important functions for advertising intermediaries. Firstly, when the consumer accesses the web page, tags located on the page that they may not click or cannot even see trigger the initiation of specific actions, for example, of the RTB processes by creating “a bid request” described in the section 2.4.1.²²⁷ Most importantly, by spreading the tags on many different websites, the server of the tag can also combine the cookies placed on them and link the data collected on each website to a single consumer.²²⁸ However, not all intermediaries are equally able to spread their tags across the internet, and large platforms, such as belonging to Alphabet and Meta, are most successful in tracking consumers online.²²⁹ For example, the *WhoTracks.Me* study found that Alphabet was tracking around 40% of the measured Web traffic and Meta around 15%.²³⁰ As advertising networks place third-party cookies through the websites of many different publishers, they can link the user’s behavior across all of these websites and aggregate a vast amount of data about the individual to create a comprehensive profile.²³¹

Other advertising intermediaries (smaller DSPs and SSPs) that do not hold a strong intermediary position online cannot spread their tracking code via tags. However, in response to their needs to track users, develop comprehensive profiles, increase the quality scores, and make more efficient bids in the RTB auction, the industry found a loophole in the Single Origin Policy to bypass its rules by a process called “cookie syncing” (alternatively “cookie matching”).²³² To illustrate, one consumer is given different unique identifiers (cookieIDs) by two parties – TRACKER1 and TRACKER2. If the consumer first visits TRACKER1 and then the web

²²⁵ Tags are sometimes also called as “tracking pixels”, “web bugs”, “pixel tags”, and “clear GIFs”. See Janne Nielsen, *Using Mixed Methods to Study the Historical Use of Web Beacons in Web Tracking*, 2 INT’L J. DIGITAL HUMAN. 1 (2021).

²²⁶ See Janice Sipior, Burke Ward & Rubén Mendoza, *Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons*, 10 J. INTERNET COM. 1, 4 (2011).

²²⁷ See *Web Beacon*, NAI: NETWORK ADVERTISING INITIATIVE, <https://thenai.org/glossary/web-beacon/> (last visited Jan 4, 2023).

²²⁸ See Nielsen, *supra* note 225, at 4.

²²⁹ See Veale and Zuiderveen Borgesius, *supra* note 31, at 228.

²³⁰ Arjaldo Karaj et al., *WhoTracks.Me: Shedding Light on the Opaque World of Online Tracking*, 8–9 (2019), <http://arxiv.org/abs/1804.08959> (last visited Jan 19, 2023).

²³¹ See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36, at 44.

²³² Veale and Zuiderveen Borgesius, *supra* note 31, at 229.

page of TRACKER2, TRACKER1 can include the cookieID it assigned to a consumer in the URL.²³³ This allows the tracker to link both cookies to a single user and combine the available data. Cookie syncing significantly widened the scope of tracked activity online by pooling the reach of multiple trackers.²³⁴ Average consumers visiting a website are unaware that the browser window of a website is sourced from several website servers and that numerous parties track their behavior by placing cookies, raising concerns about consumer privacy.²³⁵

In contrast to the Web, accessed via web browsers, mobile app developers traditionally had more freedom to track mobile users via mobile advertising identifiers (MAIDs).²³⁶ The most prevalent MAIDs in the EU are Google Advertising ID (GAID), which is placed on the Android operating system and was installed on 69% of mobile devices in 2022, and Apple Identifier for Advertisers (IDFA) on iOS, installed on 30% of devices.²³⁷ In the Android ecosystem, one study found that Alphabet tracked 88.4% of the mobile apps and Meta 33.9%.²³⁸ Empirical studies for analyzing tracking in mobile apps in the Apple iOS system are scarce.²³⁹ Lastly, third-party apps and plug-ins have a variety of ways to access the unique identifiers of mobile devices, such as phone numbers, SIM numbers, or MAC addresses.²⁴⁰ Such a variety of identifiers are also used to link a mobile device to other devices (e.g., desktop computers), as providing OBA is among several purposes of cross-device tracking.²⁴¹

2.4.3. Cookieless OBA

Due to the concerns about consumer privacy, reliance on cookies and MAIDs for OBA is a highly controversial and heavily regulated practice. The EU privacy and data protection law sets high standards for cases in which processing data via trackers can be considered lawful (Section 6.1.2). It is increasingly difficult for advertising intermediaries to place third-party advertising cookies legitimately. Partly due to the pressure from the regulators, web browsers and device manufacturers started to move away from OBA based on third-party tracking.

²³³ URL may look like <http://tracker2.com?tracker1cookieID=mv&fzb228>. *Id.* at 228.

²³⁴ 53 companies observe more than 91% browsing behavior of all internet users. *Id.* at 229.

²³⁵ *See Id.* at 229–230.

²³⁶ *See Id.* at 229.

²³⁷ European Commission Study Recent Digital Advertising Developments, *supra* note 36 at 41.

²³⁸ *See* Reuben Binns et al., *Third Party Tracking in the Mobile Ecosystem*, in PROCEEDINGS 10TH ACM CONF. ON WEB SCI. 23 (2018), <http://arxiv.org/abs/1804.03603> (last visited Jan 19, 2023).

²³⁹ *See* Veale and Zuiderveen Borgesius, *supra* note 31, at 229.

²⁴⁰ *See Id.* at 8.

²⁴¹ *See* Sebastian Zimmeck et al., *A Privacy Analysis of Cross-Device Tracking*, in PROCEEDINGS 26TH USENIX SECURITY SYMPOSIUM IS SPONSORED BY USENIX (2017).

In 2019, Mozilla’s Firefox adopted a default configuration to disable third-party cookies for advertising unless activated by the user, and in 2020, a similar feature was adopted by Apple’s Safari.²⁴² Despite owing much of its financial success to third-party cookies, Alphabet announced that Chrome—which has 65% of the web browser market²⁴³—would follow Firefox and Safari in disabling third-party cookies as the default configuration in 2023.²⁴⁴ However, Alphabet later announced that it would delay the phase-out until the second part of 2024.²⁴⁵ Similar dynamic is unfolding for the mobile trackers. In 2021, Apple introduced the App Tracking Transparency Framework, which disabled a default possibility to track third-party apps for advertising purposes, which has caused considerable disruption to the OBA markets.²⁴⁶ Meta was particularly affected by these changes – its stock price dropped 26% as it anticipated a \$10 billion loss in revenue.²⁴⁷

As the OBA industry is forced to move away from tracking based on third-party cookies, it started looking for other ways to connect users with their browsing records to compile their behavioral profiles.²⁴⁸ “Device fingerprinting” is one such method by which seemingly insignificant information about the features of the device, such as screen resolution and the list of installed fonts, are analyzed to give the device a unique “fingerprint”.²⁴⁹ This fingerprint can be used, for example, to

²⁴² See Marissa Wood, *Today’s Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, THE MOZILLA BLOG (Sep. 3, 2019), <https://blog.mozilla.org/en/products/firefox/firefox-news/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/> (last visited Jan 5, 2023). See Nick Statt, *Apple Updates Safari’s Anti-Tracking Tech With Full Third-Party Cookie Blocking*, THE VERGE, Mar. 24, 2020, <https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking> (last visited Jan 5, 2023).

²⁴³ See *Browser Market Share Worldwide*, STATCOUNTER GLOBAL STATS, <https://gs.statcounter.com/browser-market-share> (last visited Jan 5, 2023).

²⁴⁴ See Dieter Bohn, *Google Chrome Third-Party Cookies Block Delayed Until 2023*, THE VERGE, Jun. 24, 2021, <https://www.theverge.com/2021/6/24/22547339/google-chrome-cookiepocalypse-delayed-2023> (last visited Jan 5, 2023). See Matt Burgess, *Google Has a New Plan to Kill Cookies. People Are Still Mad*, WIRED, Jan. 27, 2022, <https://www.wired.com/story/google-floccookies-chrome-topics/> (last visited Jan 5, 2023).

²⁴⁵ See Kyle Wiggers, *Google Delays Move Away from Cookies in Chrome to 2024*, TECHCRUNCH, Jul. 27, 2022, <https://techcrunch.com/2022/07/27/google-delays-move-away-from-cookies-in-chrome-to-2024/> (last visited Jan 19, 2023). See Anthony Chavez, *Expanding Testing for the Privacy Sandbox for the Web*, GOOGLE: THE KEYWORD (Jul. 27, 2022), <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> (last visited Jan 19, 2023).

²⁴⁶ See Jacob Loveless, *Council Post: How Does Apple’s App Tracking Transparency Framework Affect Advertisers?*, FORBES, Aug. 22, 2022, <https://www.forbes.com/sites/forbesbusinesscouncil/2022/08/22/how-does-apples-app-tracking-transparency-framework-affect-advertisers/> (last visited Jan 5, 2023).

²⁴⁷ See Daniel Newman, *Apple, Meta And The \$10 Billion Impact Of Privacy Changes*, FORBES, Feb. 10, 2022, <https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/> (last visited Jan 19, 2023).

²⁴⁸ See Zard and Sears, *supra* note 1, at 816.

²⁴⁹ See *Cover Your Tracks*, ELECTRONIC FRONTIER FOUNDATION, <https://coveryourtracks EFF.org/learn> (last visited Jan 19, 2023).

combat fraud (e.g., identifying a person trying to log in to a site is likely an attacker who stole the credentials), but also to track a single consumer across different websites without their knowledge and without a way of opting out.²⁵⁰ Device fingerprinting allows tracking users without cookies, but also it can be used to respawn deleted identifiers in case the consumer deletes cookies.²⁵¹ Research found fingerprinting evidence on at least 4.4%–5.5% of top websites.²⁵² However, as fingerprinting is challenging to observe, these numbers can be regarded as the lower bounds.²⁵³

While device fingerprinting provides an alternative privacy-invasive tracking practice, some initiatives have successfully demonstrated the possibility of creating consumers' behavioral profiles while preserving the confidentiality of the data. One example is the web browser *Adnostic* which, since 2010, allows the creation of a behavioral profile of users and uses them to target them with advertisements without sharing any of the data with other parties.²⁵⁴ Similar privacy-preserving OBA alternatives such as Privad, AdVeil, and Brave are slowly entering the market.²⁵⁵ Alphabet has also started an initiative called Privacy Sandbox, in which the company considers various OBA alternatives that preserve the confidentiality of data – that is, not share data with third-party providers. One such alternative that was shelved is called Federated Learning of Cohorts (FLoC).²⁵⁶ Instead of assigning unique identifiers to the users, like in the case of cookies, using FLoC, a web browser would analyze users' browsing behavior and assign consumers to “cohorts”, i.e., clusters of consumers with similar browsing behavior and presumably similar habits and interests.²⁵⁷ Other similar approaches explored by Alphabet are Topics

²⁵⁰ See Nick Nikiforakis et al., *Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting*, in IEEE SYMPOSIUM SECURITY & PRIVACY 541 (2013), <https://www.computer.org/csdl/proceedings-article/sp/2013/4977a541/12OmNCwlalM> (last visited Jan 4, 2023).

²⁵¹ See Veale and Zuiderveen Borgesius, *supra* note 31, at 21.

²⁵² See Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, in CCS '14: PROCEEDINGS ACM SIGSAC, <https://dl.acm.org/doi/epdf/10.1145/2660267.2660347> (last visited Jan 4, 2023).

²⁵³ See Veale and Zuiderveen Borgesius, *supra* note 31, at 230.

²⁵⁴ See Vincent Toubiana et al., *Adnostic: Privacy Preserving Targeted Advertising*, in PROCEEDINGS OF THE NETWORK AND DISTRIBUTED SYSTEM SYMPOSIUM (March 2010), <https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf>. See also *Adnostic: Privacy Preserving Targeted Advertising*, ADNOSTIC, <https://crypto.stanford.edu/adnostic/> (last visited Jan 19, 2023).

²⁵⁵ See Micah Altman et al., *Practical Approaches to Big Data Privacy over Time*, 8 INT'L DATA PRIVACY L. 29 (2018). See European Commission Study Recent Digital Advertising Developments, *supra* note 36, at 157.

²⁵⁶ See *Federated Learning of Cohorts (FLoC)*, THE PRIVACY SANDBOX, <https://privacysandbox.com/proposals/floc/> (last visited Jan 19, 2023).

²⁵⁷ *Id.*

API²⁵⁸ and FLEDGE.²⁵⁹ These approaches aim at replacing functionality served by cross-site tracking but maintain detailed lifestyle targeting of OBA.²⁶⁰ Using Privacy Sandbox alternatives for OBA can mitigate personal data breach and confidentiality concerns, but it is likely to not be able to address concerns about consumer manipulation and exploitation in general. The industry is moving away from OBA based on third-party tracking into browser-based or local OBA, further centralizing power in advertising markets with large platform providers.

2.5. Conclusion: Online Behavioural Advertising

This section summarizes Chapter 2 to answer the first sub-question of the thesis:

SQL1: what is online behavioral advertising (OBA)?

Online behavioral advertising (OBA) is an online phenomenon that involves showing consumers advertisements that are personalized based on their behavioral data. OBA has three cumulative components: (i) advertisement is targeted to individual consumers, (ii) targeting is based on the consumers' observed behavior, and (iii) consumer behavior is observed *and/or* the consumer is targeted online. OBA reflects the advertising paradigm based on three premises: (i) targeting individual consumers with advertisements is beneficial for advertisers and possibly consumers, (ii) observed consumer behavior reveals what a consumer reacts to better than surveying, and (iii) the Internet can be used to observe and influence consumer behavior.

OBA can be understood as one of several configurations of online advertising that actualizes this paradigm. As a configuration, OBA is a particular form of online personalized advertising that entails targeting an individual consumer sorted into segments based on interests ("surf enthusiast") or detailed demographic traits ("household income top 10%") that AI systems inferred based on behavioral data about the consumer. Consumer behavioral data may include, among others, consumer Web browsing or social media behavior, mouse cursor movements, geo-location, or keyboard strokes.

Typically, publishers offer OBA configuration to advertisers on their online advertising dashboards. Platform providers such as Alphabet and Meta are the most prominent publishers allowing advertisers to advertise on websites and apps

²⁵⁸ See *Topics API overview*, CHROME FOR DEVELOPERS (2022), <https://developer.chrome.com/docs/privacy-sandbox/topics/overview/> (last visited Oct 11, 2023).

²⁵⁹ See Altman et al., *supra* note 255; See European Commission Study Recent Digital Advertising Developments, *supra* note 36, at 157.

²⁶⁰ See Shanika Wickramasinghe & Miklos Zoltan, *A Complete Guide To Google FLoC - What It Does and How It Works - How FloC Affects Privacy*, PRIVACY AFFAIRS (Apr. 25, 2023), <https://www.privacyaffairs.com/google-floc/> (last visited Jan 19, 2023).

provided by other publishers that join their networks (e.g., Google Display Network, Meta Audience Network). These advertising networks are closed ecosystems where platforms control OBA sales and are called “walled gardens”. Google dominates the search advertising market, and Meta dominates the social media advertising market. Google also dominates open exchange intermediation for display advertising, where all networks and publishers compete for advertising spaces over the Internet.

To execute OBA configurations, platforms, publishers, intermediaries, and networks, track consumers over the Internet, and compete in real-time bidding (RTB) auctions. RTB is typically won by the party with the most data about the consumer, resulting in competition in extracting consumer data. In sum, OBA is a configuration of online advertising that requires the processing of consumer behavioral data that platforms are most well-positioned to collect and monetize. The interest of platforms that advertisers select OBA between different advertising configurations results in cementing the online infrastructure for consumer surveillance in the online environment. The industry is moving away from OBA based on third-party tracking into browser-based or local OBA, further centralizing power in advertising markets with large platform providers.

CHAPTER 3. MANIPULATION

This thesis evaluates the ability of the European Union (EU) legal framework to safeguard against consumer manipulation harms of online behavioral advertising (OBA). In order to explain how OBA leads to consumer manipulation harms, the thesis builds a coherent theory of manipulation. With this aim in mind, this chapter answers the second sub-question of the thesis:

SQ2: what is manipulation?

Section 3.1 describes influences on human behavior and delineates manipulation from other forms of influence. Section 3.2 defines the concept of vulnerability in the context of decision-making that can be exploited for manipulation. Section 3.3 applies the understanding of layered vulnerability to describe different levels of an influence being manipulative. Section 3.4 concludes by formulating an answer to SQ 2.

3.1. Influencing Human Behavior

This section identifies characteristics of manipulation that distinguish it from other forms of influence. Section 3.1.1 places manipulation in the context of influences on human behavior, section 3.1.2 defines forms of influence such as coercion and persuasion and delineates them from manipulation, and section 3.3.3 expands on the defining characteristics of manipulation as a form of influence.

3.1.1. Influence

To *manipulate* something means to move it or to control it.²⁶¹ One can manipulate technical instruments, for example, a computer with a keyboard or a car with a steering wheel.²⁶² One can also manipulate animals—for example, snakes can be manipulated to mimic dancing (“snake charming”).²⁶³ Similarly, one can manipulate human beings—they can be moved and controlled as if they were a computer or a snake.²⁶⁴ This thesis talks of manipulation as a form of influence on human behavior. Manipulation can also be understood as a form of influence that radically re-conditions the target’s behavior.²⁶⁵ As an illustrative analogy, behavioral scientist B.F. Skinner successfully conditioned the behavior of pigeons to play a version of ping pong.²⁶⁶ This thesis differentiates the application of such strategies on human beings from ordinary interpersonal forms of manipulation and explicitly refers to it as “global manipulation”.²⁶⁷

In ordinary discussions, *manipulation* as a form of influencing human behavior is morally loaded and conveys a derogatory connotation. In interpersonal relationships, manipulators are said to influence someone’s behavior through a “guilt trip” – making someone feel guilty, “peer pressure” – making someone fear social disapproval, “negging” – making someone feel bad about themselves, “emotional blackmail” – making someone fear the withdrawal of affection, or

²⁶¹ Manipulate, BRITANNICA DICTIONARY, <https://www.britannica.com/dictionary/manipulate> (last visited Jan 24, 2023).

²⁶² See Susser, Roessler, and Nissenbaum, *supra* note 38, at 12.

²⁶³ See *Snake Charming*, WIKIPEDIA (2023), https://en.wikipedia.org/wiki/Snake_charming (last visited Jan 31, 2023).

²⁶⁴ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 12.

²⁶⁵ See Robert Noggle, *The Ethics of Manipulation*, in THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY 1.1 (Edward N. Zalta ed., Summer 2022), <https://plato.stanford.edu/archives/sum2022/entries/ethics-manipulation/> (last visited Jan 25, 2023).

²⁶⁶ See Marina Koren, *B.F. Skinner: The Man Who Taught Pigeons to Play Ping-Pong and Rats to Pull Levers*, SMITHSONIAN MAGAZINE (Mar. 20, 2013), <https://www.smithsonianmag.com/science-nature/bf-skinner-the-man-who-taught-pigeons-to-play-ping-pong-and-rats-to-pull-levers-5363946/> (last visited Jun 28, 2023).

²⁶⁷ Famous fictional depictions of global manipulation include: See e.g., ALDOUS HUXLEY, BRAVE NEW WORLD (1932). See e.g., A CLOCKWORK ORANGE (Warner Bros., 1971). See e.g., THE MATRIX (Warner Bros., 1999).

“seduction” – making something seem (sexually) appealing.²⁶⁸ In philosophical discussions, there is little agreement on what binds these forms of influences together — what are the necessary and sufficient conditions for a practice to be identified as manipulation (i.e., identification question), and what makes manipulation wrong (i.e., evaluation question).²⁶⁹

Consequently, legal and policy discussions are contaminated by the variety of subjective moral standpoints one can adopt about manipulation, making it challenging to define malicious practices, identify their harms, assign responsibility, and tailor regulatory intervention.²⁷⁰ This thesis aims to provide a coherent framework for understanding manipulation that can help evaluate the extent to which OBA may lead to this outcome.²⁷¹ The harms of manipulation, and therefore, the extent to which it requires regulatory intervention, are addressed separately in Chapter 5. Aiming to capture the concept of manipulation in a way that makes it useful in policy discussions, this chapter steps away from normative evaluations as much as possible and approaches the concept from a purely analytic point of view, attempting to describe it as a particular type of influence.²⁷²

3.1.2. Persuasion, Coercion, and Manipulation

As social creatures, humans depend on each other for almost everything they need, and to get those needs met, they influence each other in various ways.²⁷³ In this sense, influence on human behavior can be understood in two dimensions: by observing what is being modified (*change*)²⁷⁴ and by observing the effect of the modification on the target (*effect*).²⁷⁵ Figure 3:1 illustrates the intersections of these dimensions in a quadrant (*quadrant of influence*). Firstly, in order to influence the target, an agent may change (*i*) the target’s understanding of options (*perception*) or

²⁶⁸ See Noggle, *supra* note 265.

²⁶⁹ See *Id.* at 1.3.

²⁷⁰ See e.g., European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 40.

²⁷¹ See generally MANIPULATION: THEORY AND PRACTICE, *supra* note 74. See CASS R. SUNSTEIN, THE ETHICS OF INFLUENCE (2016). See Robert Noggle, *Pressure, Trickery, and a Unified Account of Manipulation*, 3 AM. PHILOS. Q. 241 (2020). See Noggle, *supra* note 265. THE PHILOSOPHY OF ONLINE MANIPULATION, *supra* note 74. See Susser, Roessler, and Nissenbaum, *supra* note 38 at 17.

²⁷² See also Allen W. Wood, *Coercion, Manipulation, Exploitation*, in MANIPULATION: THEORY AND PRACTICE 18–21 (Christian Coons & Michael Weber eds., 2014).

²⁷³ See *Id.* at 17. See also Christian Coons & Michael Weber, *Introduction: Manipulation: Investigating the Core Concept and Its Moral Status*, in MANIPULATION: THEORY AND PRACTICE , 1 (Christian Coons & Michael Weber eds., 2014). See also PLATO, REPUBLIC 59 (2008).

²⁷⁴ Words formatted in *Italics* inside the parenthesis refer to how the concepts appear in Figure 3:1

²⁷⁵ This view is based on dichotomy proposed by Susser, Roessler, and Nissenbaum. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 14. In this thesis, “options” relate to “decision-space” and “perception” to “decision-making process”.

(ii) the target’s options (*options*).²⁷⁶ Second, the effect of the change may be that the target of the influence has (a) acceptable alternative options (*choice*) or (b) no acceptable alternative options or no ability to exercise choice between them (*no choice*).²⁷⁷ This thesis uses the model illustrated by Figure 3:1, to delineate between different forms of influences, in particular persuasion with reason (quadrant [i][a]), persuasion with incentives (quadrant [ii][a]), coercion (quadrant [ii][b]), and manipulation (quadrant [i][b]). This chapter explains each of these forms of influences and provides illustrative (but non-exhaustive list of) examples (*examples 1–12*) that are also placed in Figure 3:1 to illustrate differences.

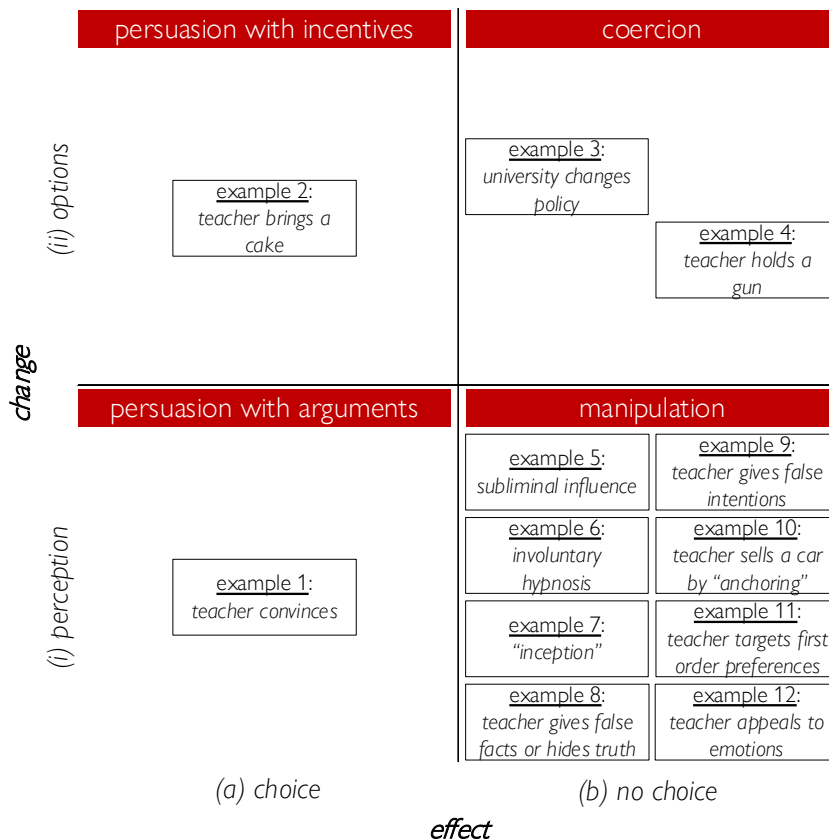


Figure 3:1. Quadrant of influence with examples (by author)²⁷⁸

Persuasion is defined as an attempt to influence targets by giving them reasons they can evaluate through conscious deliberation.²⁷⁹ One can provide these reasons

²⁷⁶ See *Id.* at 14-17.

²⁷⁷ See *Id.* at 14-17.

²⁷⁸ The figure is the author’s representation of a theory of influences developed by Susser, Roesler, and Nissenbaum. See generally *Id.*

through rational argumentation (i.e., rhetoric) or through incentives.²⁸⁰ In the first case, this amounts to an attempt to change the target’s perception of options, and in the latter, changing the target’s options. Nevertheless, persuasion is a form of influence that openly appeals to the target’s capacity for conscious deliberation and leaves the target with acceptable alternative options.²⁸¹

In example 1,²⁸² a university teacher wants students who have not been exposed to the *Covid-19* virus to attend class in person during a pandemic. The teacher explains why students should come to class by providing arguments. The teacher argues that in-class sessions build better rapport enable a more natural flow of interaction and that as the university facilitates hybrid education and high standards of health safety requirements, students should come to class, although they can join the class online. In this case, the teacher persuades the students with arguments – attempting to change their understanding of the options without changing available options (quadrant [i][a]). In example 2, on top of the arguments, the teacher also announces that an after-class chocolate cake will be provided for the students attending the session in class. In this case, the teacher persuades by offering a chocolate cake as an incentive – attempting to reconfigure students’ options but leaving acceptable alternatives. While chocolate cake can be an attractive incentive, it cannot be regarded as irresistible (quadrant [ii][a]).²⁸³

Providing irresistible incentives can be considered a form of *coercion* – as it reconfigures the target’s options, so that there are no acceptable alternatives (quadrant [ii][b]).²⁸⁴ If persuasion equates to “making an offer”, coercion can be understood as “making an offer that one cannot refuse”.²⁸⁵ In example 3, the teacher announces the new university policy and requests all students who have not been exposed to the virus to come to class in person, stating that all students attending the session online without medical evidence of exposure will be marked as “absent”. In this case, the teacher prompts students by taking away an acceptable alternative, that

²⁷⁹ Generally, persuasion can be understood in two ways: in the broader sense, the term persuasion is an umbrella term for all forms of influence, from rhetoric to violent coercion. This thesis uses the term in its narrow sense, meaning “changing someone’s mind by giving reasons he or she can reflect and evaluate.” *Id.* at 13–17.

²⁸⁰ *Id.* at 14.

²⁸¹ *Id.*

²⁸² Underlined examples are placed in Figure 3:1.

²⁸³ Rudinow formulates persuasion by providing “resistible incentives”. See Joel Rudinow, *Manipulation*, 88 *ETHICS* 338, 342 (1978). See also Susser, Roessler, and Nissenbaum, *supra* note 38 at 15.

²⁸⁴ Susser, Roessler, and Nissenbaum, *supra* note 38 at 15.

²⁸⁵ Making “an offer someone cannot refuse” is a catchphrase of Vito Corleone, a fictional mafia don in the movie “The Godfather”. See *THE GODFATHER* (Paramount Pictures, 1972). See Susser, Roessler, and Nissenbaum, *supra* note 38, at 14.

is, joining the class online without repercussions. Therefore, coercion can be defined as an overt influence that leaves the target with no acceptable alternatives.²⁸⁶

Similar to manipulation, this thesis refers to coercion in its non-moral sense. The moral and legal validity of coercion is context-dependent.²⁸⁷ For instance, educational institutions are usually authorized to force students to attend class, and within the entire EU, police officers have the authority to use violence to coerce people into specific behavior, including putting them in jail. Coercion contrasts with persuasion through incentives in that it takes away acceptable alternatives. While a coerced person can physically choose an alternative, not attend the class, or run away from the police, these alternatives cannot be regarded as acceptable due to some extent to the likelihood of failure and the high severity of their consequences, such as being delisted by the education institution or being shot by police officers.²⁸⁸

Coercion and persuasion with incentives are similar in that they reconfigure the options available for the target and appeal to the target's capacity to deliberate consciously on these reconfigured options.²⁸⁹ In other words, persuaders and coercers make their influence explicit and overt to encourage their targets to deliberate on their best interests. In example 4, a university teacher holds a student at gunpoint and demands that they come to class. In this case, a teacher with a gun wants the student to be consciously aware of two options: attending a class or giving away their life. While a coercer is one who modifies options in a way that a choice between alternatives is irresistible, a target of coercion is ultimately one who evaluates the worth of their time in class against the worth of their life and consciously takes a decision accordingly.²⁹⁰

²⁸⁶ See *Id.*; Wood, *supra* note 272 at 17.

²⁸⁷ See Wood, *supra* note 272 at 34.

²⁸⁸ What is acceptable depends on the moral standpoint of an individual. For example, for Plato death is more acceptable than losing freedom. See PLATO, *supra* note 273, at 81. Likewise, stoic philosophers have long argued that death is an acceptable option and that "choice" can never be lost. See e.g., EPICETUS, DISCOURSES, FRAGMENTS, HANDBOOK 81 (2014). Such understandings of human choice are aspirational, and are not found in legal framework. See about "irresistible incentives" Rudinow, *supra* note 283, at 341.

²⁸⁹ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 15.

²⁹⁰ *Id.* at 16. Some philosophers argue that coercion not only makes the target aware of the influence and the options, but that coercer wants the coerced to be *rational*. See e.g., Coons and Weber, *supra* note 273, at 15. This argument can be defended only to some extent. Holding someone at gunpoint, in most instances, primarily appeals to the target's emotions rather than rationality. Purely rational analysis can allow a target to calculate the likelihood of other acceptable options (e.g., it is easy to overpower the coercer, or there is a possibility to run away). Nevertheless, a target typically makes a decision based on their fear of which the target is acutely aware. Therefore, this thesis does not argue that coercion appeals to rationality per se but conscious awareness. Similarly, this thesis argues that manipulation subverts conscious deliberation (not rationality), a self-aware decision-making process. See also Susser, Roessler, and Nissenbaum, *supra* note 38, at 16.

In contrast to persuasion and coercion, manipulation is a form of influence that “subverts” the target’s capacity to deliberate on available options consciously (quadrant [i][b]).²⁹¹ In other words, manipulation displaces a target of influence as an agent who makes a conscious decision.²⁹² In manipulation, a target of influence acts like a puppet whose strings are being pulled by someone else.²⁹³ A university teacher can be said to manipulate students when a teacher places “subliminal”²⁹⁴ messages in the presentation that successfully influence students to come to class (example 5). The same would be true if a teacher induces an involuntary hypnotic state (example 6) to convince students or relies on sophisticated technology to “incept” an idea of coming to class while they are asleep (example 7).

It rarely (if ever) happens that manipulative influence completely bypasses the target’s conscious deliberation process.²⁹⁵ Even in subliminal influence (example 5), involuntary hypnosis (example 6), or “inception” (example 7),²⁹⁶ where stimulus bypasses conscious deliberation entirely, a target maintains some agency in their decision-making process.²⁹⁷ Instead, during manipulation, to steer a target towards their end, an agent inserts themselves into the target’s decision-making process in a way that stays hidden from the target.²⁹⁸ By hiding the influence, manipulation alters the target’s perception of available options. As the target cannot consider the

²⁹¹ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 16. In particular, this thesis agrees that the salient issue is whether or not the influence appeals to target’s conscious awareness, not rationality.

²⁹² *Id.* at 16.

²⁹³ See *Id.* at 17. According to authors, when the manipulative influence is found out, a target feels “played” in contrast to coercion when a target feels “used”.

²⁹⁴ “Subliminal stimuli” refers to visual, audible or any other sensory stimuli below the threshold for conscious perception. While effects of subliminal stimuli on human behavior is disputed, some studies find that such stimuli can affect decision-making processes. See S. J. Brooks et al., *Exposure to Subliminal Arousing Stimuli Induces Robust Activation in the Amygdala, Hippocampus, Anterior Cingulate, Insular Cortex and Primary Visual Cortex: A Systematic Meta-Analysis of fMRI Studies*, 59 *NEUROIMAGE* 2962 (2012). (“[D]ata suggest that despite stimulus presentation being presented outside of conscious awareness, the brain remains able to respond to such stimuli, mainly in sub-cortical regions associated with bodily arousal, implicit memory, conflict monitoring and detection of unpredictability. Activation in these brain regions, using subliminal paradigms, provides robust evidence that specific arousal systems in the brain can be activated outside of conscious awareness.”)

²⁹⁵ See SUNSTEIN, *supra* note 271 at 82. See also Shaun B. Spencer, *The Problem of Online Manipulation*, 3 *UNIV. ILL. L. REV.* 960, 990 (2020). See Susser, Roessler, and Nissenbaum, *supra* note 38 at 17.

²⁹⁶ See *INCEPTION* (Warner Bros., 2010). Thanks to Agata Szczepańska for suggesting this example.

²⁹⁷ See SUNSTEIN, *supra* note 271 at 82. See Coons and Weber, *supra* note 273 at 6.

²⁹⁸ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 17. This account of manipulation has been criticized because of ambiguity about exactly what remains hidden. See SUNSTEIN, *supra* note 271 at 102–107. Sunstein argues that the issue is that the influence does not “sufficiently” appeal to conscious deliberation. Sunstein focuses on “manipulative practices” as attempts of manipulation not on “manipulation” that is a successful outcome of manipulative practices addressed by Susser, Roessler, and Nissenbaum.

influence as part of evaluating the options, it takes away from their ability to exercise choice.²⁹⁹

3.1.3. Manipulation: Hidden, Successful, Intentional Influence

In summary, manipulation can be understood as a *hidden influence* on human behavior. The manipulator hides something important from the target.³⁰⁰ While some forms of manipulation, for example, subliminal influence (example 5), may hide the manipulative stimulus itself, other forms may make the stimulus visible but hide the manipulator's role or intentions (example 8, example 9). In example 8, the university teacher refers to the new university policy to announce that all students attending the session online without medical evidence of exposure to the virus will be marked as "absent". However, unlike example 3, university policy has not been changed, yet the teacher hides that students are not obligated to attend class. This scenario is an example of *deception*, a specific type of manipulation. Students are aware of the stimulus: the teacher wants them to be in class. However, they are unaware that the teacher is giving them false information by referring to a non-existing policy and that students are, in fact, not required to attend the class in person. Therefore, the teacher's role and the mechanism of influence remain hidden from the students.

As soon as a target of influence becomes aware of a covert influence, influence becomes part of their decision-making.³⁰¹ For example, once students become aware that the teacher shared false information and that university policy allows them to voluntarily choose between in-class and online attendance, they face a different set of acceptable options. In example 9, when students confront the teacher, the teacher admits that they did not have the authority to demand in-class attendance but tells them that they resorted to announcing it anyway because coming to class is in the student's best interests, and this was the only way they could convince them. This time, the teacher does not disclose that the scarcity of students in the class makes it difficult for the teacher to concentrate. Therefore, the teacher hides some part of the intention or a reason for the influence, again classifying the influence in example 9 as deception and, thus, manipulation.

Manipulation is not limited to deception, including hiding stimulus (example 5), falsifying facts (example 8), or hiding intentions (example 9); it can also be a

²⁹⁹ Even in retrospective analysis, when assessing how a person made a decision, it can be complicated to understand if the manipulator influenced them (and to what extent). The question arises: is it ever possible to be sure that the target would make a different decision without manipulative influence? Such certainty is not required for defining manipulation. On the contrary, uncertainty about forming a decision can be seen as an element of manipulation. People who "feel manipulated" can not fully understand why they acted the way they did or if they did so in their or someone else's best interests. See also Susser, Roessler, and Nissenbaum, *supra* note 38, at 17.

³⁰⁰ See SUNSTEIN, *supra* note 271, at 102.

³⁰¹ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 20.

form of pressure, in which manipulator is hiding psychological mechanisms by which a stimulus steers the target's behavior (section 3.2).³⁰² That being said, manipulation is always *intentional*.³⁰³ Exaggerated portrayals of manipulators include depicting them scheming with an evil smile or laughter.³⁰⁴ Nevertheless, manipulation does not always involve conscious deliberation to hide some aspect of influence and exploit vulnerability.

In essence, manipulation can occur when a manipulator elects to influence a target and neglects to deliberate the means through which influence is achieved.³⁰⁵ In other words, for influence to be classified as manipulation, the *intention* to influence must always be present, but the hiddenness of influence can be caused by negligence.³⁰⁶ For example, negging involves an attempt to influence another person's behavior by making that person feel bad about themselves or the situation. In intimate, friend, and family relationships, people do not always deliberately mean to make others feel bad but might do so anyway and somewhat unconsciously to compel them to do something. Such dual nature of manipulation as deception and hidden pressure comes back throughout later sections of the thesis (e.g., section 3.2).

Manipulation is also a "success concept" – it reflects that the stimulus hiddenly and successfully influenced a target towards an outcome.³⁰⁷ Manipulation itself is blind to the methods and strategies; instead, it suggests that intentional influence has taken place in a way that remained hidden from the target of this influence.³⁰⁸ There are no degrees in manipulation: it has either occurred or not. In contrast, a practice can be *manipulative* if it is an attempt to manipulate, whether or not such an attempt is successful, and, thus, leads to manipulation.³⁰⁹

For example, in the previously mentioned example 9, if students had recognized that their teacher did not disclose their true intentions, there would be no case of manipulation: students would deliberate on the true intentions of the teacher (*i.e.*, that he could not concentrate without students attending class in person) and decide whether they wanted to join in person or not. Nevertheless, the teacher's

³⁰² See Spencer, *supra* note 295, at 990.

³⁰³ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 26.

³⁰⁴ See e.g., Heath Ledger's depiction of "Joker" in Christopher Nolan's "The Dark Knight". See THE DARK KNIGHT (Warner Bros., 2008).

³⁰⁵ The account of manipulation as "careless influence" was first developed by Klenk. See Michael Klenk, (*Online*) *Manipulation: Sometimes Hidden, Always Careless*, 80 REV. SOC. ECON. 85, 13 (2022). Klenk argues that an action is manipulative if "a) M[anipulator] aims for S[subject] to do think, or feel b through some method m and b) M disregards whether m reveals eventually existing reasons for S to do, think or feel b to S"). See also Noggle, *supra* note 265. Klenk explicitly states to disagree with the view that manipulation is hidden.

³⁰⁶ See *Id.*

³⁰⁷ See Note 298.

³⁰⁸ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 27. See Wood, *supra* note 272, at 11.

³⁰⁹ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 27.

actions would still be manipulative because an aspect of the influence intentionally hidden can still be regarded as manipulative, as he attempted to manipulate the students but failed to do so.

Therefore, this thesis defines manipulation as:

*Agent's successful and intentional attempt to influence the target's behavior where an essential aspect of an influence remains hidden from the target and an agent is aware that the method of influence is likely to exploit the target's decision-making vulnerabilities.*³¹⁰

In summary, when the target acts towards the agent's desired outcome, the agent has manipulated the target if:

- 1) the agent intended to influence a target towards an outcome;
- 2) an essential aspect of an influence remains hidden from the target and
- 3) the agent is aware that the method of influence is likely to exploit the target's decision-making vulnerabilities.

This thesis aims to define manipulation in a helpful way for policymakers and enforcers. As policy may entail preventing manipulation from occurring, it is essential to evaluate not only the situations that can be evaluated as successful manipulation but also manipulative practices that may remain unsuccessful. With this in mind, Section 3.2 further elaborates on methods of manipulation, and Section 3.3 formulates the way to measure the “manipulativeness” of an agent's attempts to influence a target. While essential aspects of influence are context-dependent, section 4.1.1 elaborates on some of those aspects in the context of advertising.

3.2. Methods: Exploitation of Vulnerability

There are various ways one can conceptualize how a manipulator manages to exert hidden influence on their target. This thesis adopts the framing closely aligned with Susser, Roesler, and Nissenbaum's view that the various means of manipulation, such as deception or pressure, can be summarized as methods that exploit human decision-making *vulnerabilities*.³¹¹ This section defines and describes

³¹⁰ Manipulation as *hidden influence* is one of at least three ways manipulation can be understood. Other two ways include manipulation as *trickery* (deception) and manipulation as *pressure*. See Noggle, *supra* note 265.

³¹¹ This thesis also refers to “exploitation” in non-moralized sense to describe that a vulnerability is used by an agent of influence towards agent's pre-determined end. See Wood, *supra* note 272, at 43. Deception essentially exploits vulnerability of “unavailability of perfect information” in human decision-making context, and pressure, generally, exploits the need for social approval. Susser, Roesler, and Nissenbaum combine all means of manipulation under the umbrella of “cognitive,

what these vulnerabilities are and how their exploitation leads to manipulation. Section 3.2.1 addresses cognitive biases, and section 3.2.2 other vulnerabilities that manipulators exploit.

3.2.1. Cognitive Biases

One way to understand the conscious deliberation process through which humans make decisions is by the interplay of a person’s beliefs, preferences, and emotions that precede their actions.³¹² Ideally, a decider would hold *beliefs* that truthfully reflect circumstances; they would form *preferences* that accurately reflect these beliefs and experience *emotions* that help them gauge their proximity to their preferences.³¹³ As people have many beliefs, desires, and emotions, conscious deliberation is a process through which one makes up one’s mind or adapts beliefs, prioritizes desires, and interprets emotions.³¹⁴ *Rationality* – a state of being governed by reason – is one form of conscious deliberation that allows a decision-maker to advance toward their self-interest by always choosing the best available option.³¹⁵

Rationality has often been an aspirational state for human beings.³¹⁶ Historically, rationality has also been ascribed to humans as their descriptive characteristic: some economic theories and legal frameworks are constructed around a view of human beings as rational beings.³¹⁷ Nevertheless, almost a century of cognitive, behavioral, and social psychology studies reveal that human beings rarely,

emotional, or other decision-making vulnerabilities”. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 26.

³¹² See Robert Noggle, *Manipulative Actions: A Conceptual and Moral Analysis*, 33 AM. PHIL. Q. 43, 4 (1996).

³¹³ See *Id.* For a simplified example to illustrate interplay of beliefs, preferences, and emotions: imagine that one believes their purpose in life is to create value for the community through their work (belief #1); they may desire to get to work constantly on time (preference #1). They feel guilty (emotion #1) when they are late. They believe that a bicycle is a faster means of transportation than being on foot (belief #2), and they feel excited (emotion #2) when considering buying a bicycle (preference #2).

³¹⁴ See *Id.* at 44–47. See generally Susser, Roessler, and Nissenbaum, *supra* note 38.

³¹⁵ R. Jay Wallace, *Practical Reason*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., Spring 2020 Edition), <https://plato.stanford.edu/archives/spr2020/entries/practical-reason/> (last visited Feb 2, 2023).

³¹⁶ *Id.* at 6.

³¹⁷ In law and economics, human beings can be imagined as economic agents who are consistently rational, and optimize for their self-interest (often referred to as “homo economicus” or “economic man”). Such views were promoted by early economic theorists, such as John Stuart Mill and Adam Smith. See e.g., JOHN STUART MILL, *ESSAYS ON SOME UNSETTLED QUESTIONS OF POLITICAL ECONOMY* (2011). See e.g., ADAM SMITH, *THE WEALTH OF NATIONS* (Robert B. Reich ed., 2000). The EU legal framework sometimes resembles such a view of humans as rational agents. For example, when referring to “average consumer” consumer protection legislation considers a consumer that is “reasonably well informed, observant, and circumspect”. See European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53, at 90.

if ever, behave entirely rationally.³¹⁸ These studies further conclude that most everyday human decision-making does not even happen consciously and deliberately.³¹⁹ Instead, they suggest that for evolutionary purposes, the human brain developed mechanisms that they call *heuristics* and *automated behavior patterns* – to shortcut the decision-making process, reduce complexity, and save energy in the face of repetitive and unimportant tasks.³²⁰

Cognitive psychologists refer to the conscious decision-making process as *System 2* and describe it as a *slow*, reflective, effortful, controlled way of thinking that requires time, energy, and attention (hereafter, *slow thinking*).³²¹ In contrast, they explain, humans make most of their decisions using the thinking paradigm they call *System 1*, which is *fast*, non-reflective, automatic, simple, and requires much less time, energy, and attention (hereafter, *fast thinking*).³²² Studies reveal that humans only mobilize slow thinking when fast thinking cannot handle the task at hand.³²³ Even then, System 1 continues to generate cues that a person receives in the form of impressions, intuitions, and feelings that they consider during their slow thinking process.³²⁴ Therefore, in many situations, these fast-thinking shortcuts are prone to errors in the decision-making process called *cognitive biases* that may lead to sub-optimal decisions.³²⁵

The “anchoring effect” is one such cognitive bias that distorts a person’s estimates by causing them to rely on a pre-existing piece of information, such as a number (an anchor) when making a decision.³²⁶ For example, presenting original/discounted prices can influence a viewer’s price perceptions. The “availability heuristic” influences a person to provide further weight to a specific scenario or an occurrence already available in a person’s memory compared to other scenarios of objectively similar weight.³²⁷ Through the “framing effect,” people

³¹⁸ Three influential works analyzing the decision-making shortcuts are: See DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011). See ROBERT B. AUTHOR CIALDINI, INFLUENCE: THE PSYCHOLOGY OF PERSUASION (Revised edition.; First Collins business essentials edition. ed. 2007); See RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: THE FINAL EDITION (Updated edition. ed. 2021).

³¹⁹ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 21.

³²⁰ See for “heuristics” Amos Tversky & Daniel Kahneman, Judgment under Uncertainty: Heuristics and Biases, 185 SCIENCE 1124 (1974). See for “automated behavior patterns” CIALDINI, *supra* note 318.

³²¹ See KAHNEMAN, *supra* note 318, at 21. Thaler and Sunstein refer to System 1 as the “Automatic System” and “Gut”, and to System 2 as the “Reflective System” and “Conscious Thought”. See THALER AND SUNSTEIN, *supra* note 318, at 19.

³²² See KAHNEMAN, *supra* note 318, at 25.

³²³ *Id.* at 24. Spencer, *supra* note 295, at 964.

³²⁴ See KAHNEMAN, *supra* note 318, at 24.

³²⁵ *Id.* at 25.

³²⁶ *Id.* at 119. See Spencer, *supra* note 295 at 964.

³²⁷ See Tversky and Kahneman, *supra* note 320, at 1128. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 22.

draw different conclusions and sometimes make contrasting decisions based on identical information framed differently.³²⁸ Also, because of the “social proof principle,” people view specific behavior as correct if they see others performing it.³²⁹ These cognitive biases can be triggered accidentally, but they are also susceptible to being exploited by an intentional external influence. In example 10 (*Figure 3:1*), a university teacher is selling his car and negotiating the price. They attempt to get the best deal by initially suggesting an inflated price and lowering it during negotiations. The initial offer acted as an anchor, and the target thought they got a good deal, even though they still paid a higher price than the car’s actual market value.

As cognitive biases are susceptible to exploitation by others, this thesis refers to them as decision-making vulnerabilities. In example 10, a target of influence is consciously deliberating, but the process is skewed, as the university teacher activates the fast-thinking brain of the buyer, introducing an influence in their conscious thinking that the target is unaware of. Alternatively, manipulators could exploit cognitive biases to bypass the conscious deliberation process altogether.³³⁰ Subliminal stimulus (example 5) or involuntary hypnosis (example 6) would be examples of such manipulation (*Figure 3:1*). Therefore, manipulation can take the form of hidden pressure that is targeted (or otherwise is likely) to exploit the target’s decision-making vulnerabilities. Being hidden is what makes such pressure a form of manipulation. If all essential aspects of influence are overt – that is, the target is aware that the influence is likely to exploit their vulnerability – an influence can be classified as *coercive*. Manipulation and coercion can be regarded as two forms of exploitation.

3.2.2. Beliefs, Desires, Emotions, and Nudges

Cognitive biases are not the only aspects of decision-making susceptible to exploitation. Human beliefs, desires, and emotions are also vulnerable to outside influences.³³¹ For example, when deciding, people can never fully cover all available information, as data that can be considered in any given situation is infinite.³³² Others may exploit this lack of perfect information to encourage their targets to hold false beliefs. Such influence on the target’s beliefs is called *deception*. Example 8 and example 9, described in section 3.1, where the university teacher provides students with false information about university policy and then

³²⁸ See Amos Tversky & Daniel Kahneman, *Rational Choice and the Framing of Decisions*, 59 J. BUS. 251, 257 (1986). See also Susser, Roessler, and Nissenbaum, *supra* note 38, at 22.

³²⁹ See CIALDINI, *supra* note 318 at xiii.

³³⁰ See Noggle, *supra* note 265.

³³¹ See Noggle, *supra* note 312, at 44. One of the earliest accounts for such a view is Plato’s *tripartite mind*: of reason, desire and passion. See PLATO, *supra* note 273, at 143–152.

³³² See Belfast Buddhist, *Alan Watts - Choice*, YOUTUBE (2016), <https://www.youtube.com/watch?v=wyUJ513hyTo> (last visited Feb 3, 2023).

about their intentions, are the paradigm examples of direct deception.³³³ Deception is always manipulation as the falsehood of the proposition is always hidden, undermining the target's ability to understand their options.³³⁴

Manipulators can also influence people's desires.³³⁵ Any given individual has a myriad of interrelated desires. A person may want to fill up their water bottle because they are thirsty, continue to work at the desk to meet their desired writing goal, and want to be outside enjoying the rare sunlight, all at the same time. Ideally, people would order these desires into preferences to maximize their self-interest.³³⁶ A person may fill up water, return to the desk immediately, and decide to go outside to enjoy some sunlight only after and if they meet their writing goal. Such orders of desires which sort out preferences about preferences are called *second-order preferences*. This ordering is rarely fully conscious and often fluid, and others can exploit this fluidity. In example 11, a university teacher is aware of their colleague's fascination with sunlight and suggests that they join them for coffee outside with the hidden intention that the colleague misses their writing goal.³³⁷ Sexual seduction is another form of manipulative influence on a target's desires.³³⁸

Human emotions also play an essential role in the decisions people make.³³⁹ Ideally, people get excited when they are about to satisfy their preferences and get

³³³ Noggle refers to "direct deception" as "any assertion of a proposition that the asserter does not believe, with the intention of causing someone to believe that the proposition is true." Noggle, *supra* note 312, at 44. Deception is largely discussed mean of manipulation. For more in depth analysis See Noggle, *supra* note 265, at 2.2.

³³⁴ See Susser, Roessler, and Nissenbaum, *supra* note 38, at 21.

³³⁵ This thesis refers to the desire to include all of the motives for acting, including visceral factors such as hunger, thirst, and sex drive, to other relatively more consciously formed preferences (e.g., attaining a law degree). Some works combine these in the word "motive". See Eric M. Cave, *What's Wrong with Motive Manipulation?*, 10 ETHICAL THEORY MORAL PRAC. 129, 130 (2007). Some framew them into "preferences" See Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 76 N.Y.U. L. REV. 630, 733–743 (1999).

³³⁶ See Hanson and Kysar, *supra* note 335, at 672.

³³⁷ It is essential here that the teacher's intentions are hidden, and the colleague is not aware that a teacher wants them to fail in their writing goal. In a way, the teacher may think they have been persuaded; they may even feel coerced – if they feel that the temptation was too much for them to handle; but as the intention is hidden, the influence is manipulation. In contrast, Noggle sees Christ's temptation by Satan as a form of manipulation. This thesis does not agree with this view. See Noggle, *supra* note 265, at 43. If we assume that Christ knows that Satan intends to make him break the fast by tempting the visceral factor of hunger, Satan provides an irresistible incentive and coerces Christ. In case Christ could resist but chose not to, then he has been persuaded. See the "martini example" in Susser, Roessler, and Nissenbaum, *supra* note 38, at 18–19.

³³⁸ For example, Cave refers to "unsavory" seduction, when a person uses cognitive biases, such as anchoring to arouse another person's sexual interest referring to Neil Straus's *The Game* and the culture of "pick-up" artists. This thesis agrees that some seduction is manipulative, but does not evaluate such manipulation is "unsavory" or not. This requires normative evaluation, that this chapter refrains from. See Eric M. Cave, *Unsavoring Seduction and Manipulation*, in MANIPULATION: THEORY AND PRACTICE, 176–177 (Christian Coons & Michael Weber eds., 2014).

³³⁹ See Noggle, *supra* note 312, at 44.

depressed when they think satisfying these preferences is impossible.³⁴⁰ In a way, emotions help humans to scan through life’s complexity to determine what to focus on.³⁴¹ For example, when a colleague follows a university teacher outside to catch some sunlight, they may feel regret, which reminds them of the second-order preference for their writing goal. However, emotions are also vulnerable to outside influence. In example 12, the colleague regrets leaving their desk and is about to return inside, but the university teacher starts to sulk about their personal life. In this case, the teacher appeals to the colleague’s sympathy and tries to get them to consider this in their deliberation process. Guilt trips, peer pressure, and emotional blackmail similarly play on people’s emotions to influence their behavior.³⁴²

Finally, human beings are also influenced by the context in which they make decisions (e.g., their physical environment).³⁴³ For example, when people decide what to buy in the cafeteria, the arrangement of options (e.g., some are at eye level, some more challenging to reach), also called “choice architecture”, influences them to select the closest options.³⁴⁴ The aspects of the choice architecture that influence people’s behavior are called “nudges”.³⁴⁵ By definition, nudges alter people’s behavior “without forbidding options or *significantly* changing their economic incentives”.³⁴⁶ Such nudges can be in the environment accidentally, but they can also be designed intentionally to influence human behavior.³⁴⁷ Many intentionally designed nudges influence to appeal to conscious deliberation (e.g., graphic health warnings on cigarette packages nudge people to consider the health effects of smoking). However, some nudges bypass conscious deliberation and influence people in a hidden way (e.g., many public bathrooms in the Netherlands introduced “fly in the urinal” that men unconsciously target and eventually minimize the spill outside the urinal). Manipulators can also nudge people by changing their decision-making contexts.³⁴⁸

In summary, humans trying to reach a decision are susceptible to manipulation in various ways: cognitive biases, beliefs, desires, emotions, and decision-making

³⁴⁰ *Id.* at 46.

³⁴¹ *Id.*

³⁴² See Noggle, *supra* note 265 at 4.2.

³⁴³ This is largely due to cognitive biases discussed in the Section 3.2.1. See generally THALER AND SUNSTEIN, *supra* note 318.

³⁴⁴ *Id.* at 1–4. Susser, Roessler, and Nissenbaum, *supra* note 38, at 23.

³⁴⁵ See THALER AND SUNSTEIN, *supra* note 318, at 6.

³⁴⁶ *Id.*

³⁴⁷ Much has been said about an overlap between nudging and manipulation. See e.g., Susser, Roessler, and Nissenbaum, *supra* note 38, at 23. See also Robert Noggle, *Manipulation, Salience, and Nudges*, 32 *BIOETHICS* 164 (2018). See also Thomas RV Nys & Bart Engelen, *Judging Nudging: Answering the Manipulation Objection*, 65 *POLIT. STUD.* 199 (2017).

³⁴⁸ Within the theory of manipulation adopted in this thesis, some nudges are not manipulative, but many are. Some manipulative nudges may lead to harm. See generally Nys and Engelen, *supra* note 347.

contexts create the vulnerabilities that manipulators can exploit to sway their targets towards their predetermined ends. Nevertheless, evaluating whether decision-making vulnerabilities have been exploited and, therefore, if manipulation has occurred is particularly challenging. This is also the case in commercial practices, such as OBA. Section 3.3. proposes how commercial practices can be investigated to evaluate whether they lead to manipulation.

3.3. Measuring Manipulativeness

In this thesis, manipulation is defined as a successful and intentional attempt to influence someone's behavior that remains hidden from the target's conscious awareness during the influence (Section 3.1). This thesis has described the exploitation of decision-making vulnerabilities, including cognitive biases, beliefs, desires, and emotions, as the means through which an agent manipulates a target (Section 3.2). Evaluating whether a particular practice manipulated a target requires concluding that it was "manipulative" and successfully affected the outcome. An influence can be considered manipulative if (1) an agent intended to direct a specific target toward a particular outcome (i.e., influence is targeted) and if (2) an agent intended or disregarded that an aspect of the influence remained hidden from the target (i.e., influence is hidden).³⁴⁹ This thesis supports the view of manipulative influence, in which an agent may overlook the hidden aspect because they are negligent towards the means through which they influence the target.³⁵⁰

However, in contrast to "manipulation", "manipulativeness" is not a binary concept; instead, it can be best imagined as a spectrum – some attempts and practices are more manipulative than others.³⁵¹ Such a degree of manipulativeness depends on the *likelihood* that targeted and hidden influence will exploit the target's decision-making vulnerabilities. When taken to a commercial context, this thesis defines manipulative practices as attempts of the business to influence a consumer towards a targeted outcome (e.g., business profit) while willing to keep some aspect of the influence hidden in a way that can exploit their decision-making vulnerabilities. Therefore, manipulative practices have three elements:

³⁴⁹ Such distinction between "manipulation" and "manipulativeness" is in line with the argumentation of Susser, Roesler and Nissenbaum. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 26–29. One deviation from their theory may be that in this thesis intentionality of manipulation does not assume *deliberateness* of hiding the influence. Such hiddenness can be due to influencer's *negligence* about the means of influence.

³⁵⁰ See generally Klenk, *supra* note 305.

³⁵¹ People often say that a person or a strategy is "very manipulative". One of the main attributes of manipulation is how far a manipulator is willing to take their influence. Let's imagine most striking examples of manipulation to illustrate this point: In the movie *Truman Show*, entire world is designed for the target (in this case protagonist) so that he has a false belief about his situation. In *Inception*, state of the art technology is precisely developed and used to hide the influence. In these cases manipulators go in great lengths to hide the influence.

- 1) they are targeted;
- 2) they are hidden, and
- 3) they are likely to exploit the target’s decision-making vulnerabilities.³⁵²

While elements (1) and (2) are essential for a practice to be considered manipulative, element (3) provides a way to measure the degree to which the practice is manipulative (Figure 3:3). In order to illustrate how the likelihood of exploitation is differential, section 3.3.1 elaborates on the distinction between labeled and layered conceptions of vulnerability; Section 3.3.2 describes different sources that layers of vulnerabilities may stem from. Section 3.3.3 illustrates how different layers of the concept of vulnerability can be used to measure degrees of manipulateness.

3.3.1. Vulnerability

In ordinary language, vulnerability means exposure to attack or damage.³⁵³ It is typically ascribed to a subject and describes relative exposure toward a particular outcome (subject *X* is vulnerable to outcome *Y*). For example, computer systems (subject) are vulnerable to cybersecurity breaches (outcome).³⁵⁴ Human beings are vulnerable to being physically or emotionally wounded (in Latin, “*vulnus*” means “wound”).³⁵⁵ Human beings are vulnerable to various types of harm, making human vulnerability a complicated concept to untangle.³⁵⁶ This is more so in legal theory, which borrows terminology and conceptual frameworks of vulnerability from

³⁵² See Susser, Roessler, and Nissenbaum, *supra* note 38, at 27.

³⁵³ See *Definition of Vulnerable*, MERRIAM-WEBSTER (2023), <https://www.merriam-webster.com/dictionary/vulnerable> (last visited Feb 6, 2023). Other definitions refer to exposure to “harm”. Harm has a specific meaning in legal discourse and is discussed in detail in Chapter 5 in the context of manipulation via OBA. To avoid confusion, this thesis refers to vulnerability as exposure to attack.

³⁵⁴ The terminology of “exploiting vulnerabilities” is widely used in cybersecurity, where it refers to hackers using vulnerabilities in computer systems to breach the security and access stored data. See e.g., *Cybersecurity Vulnerabilities: Types, Examples, and More*, GREAT LEARNING BLOG: FREE RESOURCES WHAT MATTERS TO SHAPE YOUR CAREER! (2023), <https://www.mygreatlearning.com/blog/cybersecurity-vulnerabilities/> (last visited Feb 7, 2023).

³⁵⁵ *Definition of Vulnerable*, *supra* note 353. See VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY, 4–5 (Catriona Mackenzie, Wendy Rogers, & Sandy Dodds eds., 2014). Also note, that in contrast to how it is often used in academic literature, human vulnerability in this thesis does not mean human fragility. This thesis endorses the view of humans being vulnerable like plants, not fragile like jewels: vulnerability that exposes plants (and humans) to injury is also the source of their growth. See Will Buckingham, *Vulnerability and Flourishing—Martha Nussbaum*, HIGHBROW (Oct. 26, 2017), <https://gohighbrow.com/vulnerability-and-flourishing-martha-nussbaum/> (last visited Feb 7, 2023). In a way, it can be argued that vulnerability is “antifragility” See for the concept of antifragility NASSIM NICHOLAS TALEB, ANTIFRAGILE: THINGS THAT GAIN FROM DISORDER (2013).

³⁵⁶ See Gianclaudio Maglieri & Jędrzej Niklas, *Vulnerable Data Subjects*, 37 COMPUTER L. SECURITY REV., 3–5 (2020).

various external disciplines, such as political philosophy, gender studies, and bioethics.³⁵⁷

These disciplines conceptualize vulnerability to address a broad range of problems.³⁵⁸ For example, bioethics considers the concept of vulnerability for protecting human research participants.³⁵⁹ In comparison, political theorists view it as a human condition (“la condition humaine”) that triggers state responsibility and places it at the roots of political organization.³⁶⁰ Such multiplicity of meanings and functions makes an overarching definition of vulnerability elusive.³⁶¹ This thesis scopes the use of the concept solely in a decision-making context, with a particular emphasis on commercial relationships.³⁶²

Even with such a scope, the quest for defining vulnerability may lead to stereotyping sub-populations or excluding the vulnerable from rigid taxonomies that cannot fully grasp the complexity of vulnerability in real-life.³⁶³ Nevertheless, this thesis recognizes the need to formulate a coherent way of thinking about vulnerability in a decision-making context to support legal discussions about the likelihood of manipulation and risks. Historically, legal discussions have adopted a “labeled” understanding of vulnerability that labels particular sub-populations (e.g.,

³⁵⁷ *Id.* at 3.

³⁵⁸ *Id.* at 3–5. See also VULNERABILITY, *supra* note 355, at 4–5.

³⁵⁹ Vulnerability is a foundational concept in bioethics. In particular, it arose as the need to give express consent for participation in human research. See Wendy Rogers, *Vulnerability and Bioethics*, in VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY (Catriona Mackenzie, Wendy Rogers, & Susan Dodds eds., 2013). See also Florencia Luna, *Identifying and Evaluating Layers of Vulnerability – A Way Forward*, 19 DEV. WORLD BIOETHICS 86 (2019).

³⁶⁰ See ROBERT E. GOODIN, PROTECTING THE VULNERABLE: A RE-ANALYSIS OF OUR SOCIAL RESPONSIBILITIES (1986). See also MARTHA C. NUSSBAUM, FRONTIERS OF JUSTICE: DISABILITY, NATIONALITY, SPECIES MEMBERSHIP (2007). See also Martha Fineman, *The Vulnerable Subject and the Responsive State*, 60 EMORY L. J. 251 (2010). Chapter 5 returns to vulnerability in context of political theory.

³⁶¹ Luna particularly argues against developing taxonomies of vulnerability and develops theory of vulnerability as *layers* and not *labels*. Her theory steps away from stereotyping vulnerable groups by “labeling”, and, maintains conceptual flexibility to cover variety of forms of vulnerability. See generally Luna, *supra* note 359. This thesis adopts Luna’s point of view of vulnerability as layered. However, while this thesis agrees that it is impossible to categorize reality in particular in such complex contexts as human behavior, it finds it necessary to create a taxonomy that resembles the real-life complexity of vulnerability at least more accurately than taxonomies in current legal instruments. This is particularly the case in the context of the view of vulnerability in the EU consumer protection law. See Joanna Strycharz & Bram Duivenvoorde, *The Exploitation of Vulnerability Through Personalised Marketing Communication: Are Consumers Protected?*, 10 INTERNET POLICY REV. (2021).

³⁶² Thesis analyzes the extent to which human beings are vulnerable to manipulation, and the extent to which decision-making is vulnerable to exploitation (such exploitation can come from coercion or manipulation).

³⁶³ See Luna, *supra* note 359, at 90.

minors, persons with mental disabilities) as “vulnerable groups”.³⁶⁴ Studies from other disciplines have criticized such a model and argued that membership in a group can be understood only as one of several “layers” of an individual’s vulnerability to manipulation.³⁶⁵ These layers rarely, if ever, apply in isolation to any given individual, but they interplay with each other to form a complex figure of a person’s vulnerability.³⁶⁶

Therefore, while entirely capturing and precisely measuring such complexity may be impossible, without outlining better contours of vulnerability to manipulation, legal instruments may fall strikingly short of meeting their aims and leave vulnerable individuals unprotected. This is important in the EU legal framework for OBA, where vulnerability is a key concept. For example, vulnerability plays a definitive role in regulating manipulative practices in the discussions on the Artificial Intelligence Act (AIA). In the proposal for AIA, the European Commission endorsed vulnerability as a labeled concept in Article 5, and also introduced vulnerability due to “an imbalance of power, knowledge, economic or social circumstances” in Article 7 that resembles the layered vulnerability approach.³⁶⁷ Therefore, to support the legal discussions in better capturing human vulnerability, this thesis builds upon neighboring disciplines and endorses the view of vulnerability as a layered concept.³⁶⁸ Section 3.3.1 explains how different layers interplay to create a spectrum of vulnerability.

3.3.2. Levels of Vulnerability

This section differentiates between three sources of vulnerability: (1) *intrinsic vulnerabilities* stem from the target of the influence; (2) *situational vulnerabilities* stem from the circumstances, and (3) *relational vulnerabilities* stem from the asymmetries in the relationship between a target and the agent of the influence. Such delineation of sources is intended to capture, rather than to limit, various types of vulnerability. In specific contexts, the line between sources of vulnerability may be blurred. For example, relational factors can be considered situational, and situational factors as intrinsic. Therefore, this thesis merely refers to sources to explicate the potentiality of different layers and suggests a way to measure vulnerability to

³⁶⁴ See e.g., Unfair Commercial Practices Directive, *supra* note 42; See also AI Act Proposal referring to technologies that “exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities”. See AI Act Proposal, *supra* note 52 at 13.

³⁶⁵ See Luna, *supra* note 359, at 90.

³⁶⁶ See *Id.*

³⁶⁷ The European Parliament has suggested updating the model to include other layers (e.g., socio-economic factors) See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021/0106 (COD) Draft 20-06-2023, art. 5, 7. [hereinafter AI Act Mandates].

³⁶⁸ See *Definition of Vulnerable*, *supra* note 353.

manipulation on the spectrum by adding them up. The following paragraphs expand on these three sources of vulnerability.

Firstly, the target of an influence can be intrinsically vulnerable to manipulation. In a decision-making context, on a fundamental level, all human beings are *inherently* vulnerable to manipulation.³⁶⁹ The source of inherent, intrinsic vulnerability in human decision-making is the human embodiment and their social nature.³⁷⁰ In particular, human thinking is shaped by the physiological and psychological needs that arise within their bodies, which also predisposes humans to cognitive biases (see more detail in section 3.2.1).³⁷¹ Humans need other human beings to meet many of their needs, and as they can never fully process all information available in a given situation, they need to rely on emotions and assumptions about other humans (trust others) and the world around them (have beliefs). Therefore, in this way, vulnerability is a constant condition in decision-making for all human beings.³⁷² One can think of it as a baseline to be a mentally and physically healthy adult capable of forming decisions independently in a situational vacuum.³⁷³

On top of the baseline or inherent, intrinsic vulnerability, each individual has other intrinsic traits that can make them particularly vulnerable to erroneous decision-making.³⁷⁴ Generally, such differential understanding of intrinsic

³⁶⁹ See MARIJN SAX, BETWEEN EMPOWERMENT AND MANIPULATION: THE ETHICS AND REGULATION OF FOR-PROFIT HEALTH APPS 76 (2021).

³⁷⁰ See Introduction: What Is Vulnerability, and Why Does It Matter for Moral Theory?, in VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY, 7 (Catriona Mackenzie et al. eds., 2013).

³⁷¹ *Id.*

³⁷² Vulnerability theorists also distinguish *dispositional v. occurrent* vulnerabilities that relate to the potential vulnerabilities and the fact that vulnerabilities are actualized. See *Id.* Imagine the example of the solubility of a sugar lump. Sugar has solubility – if it is placed in water, it will dissolve. However, it is not dissolved unless it is exposed to water. Similarly, there are potential and actual vulnerabilities in the decision-making context. All human beings are universally vulnerable to manipulation. This potential exists even when a person is alone in a dark room (without a phone or an internet connection). However, manipulation can only happen if a social interaction occurs. This thesis only discusses the actualized vulnerability, that is, when the target is being influenced toward a particular outcome.

³⁷³ Humans rarely make decisions in a vacuum, fully autonomously. Relationships with others often provide catalysis for human decision-making. Some philosophers call this phenomenon “relational autonomy” and understand a human being as a “relational self”. See JONATHAN HERRING, LAW AND THE RELATIONAL SELF (1 ed. 2019). Due to this relational nature some scholars see autonomy and vulnerability as *entwined*. See Joel Anderson, *Autonomy and Vulnerability Entwined*, in VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY 134 (Catorina Mackenzie ed., 2013). See also SAX, *supra* note 369, at 78. This thesis agrees with such an understanding human decision-making. It suggests that vulnerability is very tissue of autonomy. That is, autonomy in humans is contingent on vulnerability. An eye sees only when it is exposed; the “Self” expresses autonomy in society or in relation to others.

³⁷⁴ See Mackenzie et al., *supra* note 349, at 7.

vulnerability is based on different degrees of resiliency and coping ability.³⁷⁵ In a decision-making context, one such intrinsic vulnerability may come from belonging to a particular age group, such as minors or the elderly. A mental disability, such as obsessive-compulsive disorder (OCD), or chronic physical illness, such as diabetes, can be considered an intrinsic personal vulnerability to manipulation. Some intrinsic traits, such as introversion or personality type, may not make a person vulnerable to manipulation *per se* but can be triggered as a vulnerability by a particular stimulus or other circumstantial or relational factors. For situations when personality traits become actualized as vulnerabilities, this thesis considers them as personal intrinsic vulnerabilities.³⁷⁶

Secondly, some vulnerabilities are *situational* in that they stem from the particularities of the circumstances that are extrinsic to individuals.³⁷⁷ Such situational vulnerabilities can be short-lived, intermittent, or long-term and typically involve environmental, social, economic, political, and personal circumstances.³⁷⁸ Environmental circumstances, such as a pandemic or an earthquake, may significantly affect individuals' decision-making processes.³⁷⁹ For some, it may become challenging to deliberate due to political circumstances, such as riots or armed conflicts. Social factors can also have a significant effect: for example, depending on the community, having a particular race, sexual orientation, or gender may be a reason for a person's oppression, making them vulnerable to a wide range of interferences with their decision-making.³⁸⁰

Systematic racism, sexism, or homophobia may blur the line between situational and intrinsic vulnerabilities: while systematic racism is not an intrinsic state to the human condition, for some, it can feel like an "inescapable" feature of their life experience.³⁸¹ Such distinction between intrinsic and situational is even more blurred when vulnerabilities stem from personal circumstances. For example, becoming a parent, going through a divorce, losing a loved one, or losing a job are personal circumstances in which people are more susceptible to influences in their decision-making.³⁸² This thesis identifies such vulnerabilities as situational because their source is the situation, not an intrinsic trait.³⁸³ The precise delineation between intrinsic and situational vulnerabilities is not necessary for the coherence of a

³⁷⁵ *Id.*

³⁷⁶ See Strycharz and Duijvenvoorde, *supra* note 361, at 5.

³⁷⁷ See SAX, *supra* note 369, at 77.

³⁷⁸ See Mackenzie et al., *supra* note 349, at 7.

³⁷⁹ See SAX, *supra* note 369, at 78.

³⁸⁰ See *Id.*

³⁸¹ See *Id.* at 77.

³⁸² See *Id.* at 77.

³⁸³ This thesis also recognizes the need for future research in this area for better delineating between different sources, and forms of vulnerability in decision-making contexts. Developing coherent framework is essential for protection of vulnerable.

layered vulnerability framework. Instead, such conceptualization intends to capture both sources of vulnerabilities and regard them as layers that may compound and exacerbate the overall vulnerability of a target to be manipulated.

Thirdly, a person can also be vulnerable to manipulation due to the particularities of their relationship with the agent of influence.³⁸⁴ Humans are vulnerable in all relationships because humans need to trust other human beings.³⁸⁵ As Keymolen puts it: “We, as human beings, cannot exactly predict the thoughts and actions of others; they are—to a certain extent—black boxes to us and, consequently, constitute a source of insecurity.”³⁸⁶ In other words, uncertainty about others’ potential actions constitutes a form of vulnerability in a person’s decision-making capabilities.³⁸⁷ Humans are particularly vulnerable when in hierarchical relationships or relationships with information or power asymmetries.³⁸⁸ For example, in a decision-making context, vulnerability occurs in teacher-to-student, employer-employee, business-to-consumer, caretaker-patient, or similar relationships where one party has the authority or the other way sets the rules of the interaction.³⁸⁹ Therefore, relationships can act as a layer of vulnerability.

In summary, illustrating different sources of vulnerability reveals various layers that can compound one another and create varying levels of vulnerability that can be imagined on a spectrum instead of a monolithic label applied to specific groups (Figure 3:2). Every human being can be regarded as having at least a baseline level of vulnerability to manipulation (*ordinary vulnerability*). A personal trait, situational circumstance, or relational asymmetry can provide a second layer and deem a person more than ordinarily vulnerable (*vulnerable*). Vulnerabilities can compound: a personal trait, a situational circumstance, or the nature of a relationship which can act as an additional layer and create a state of *heightened vulnerability*. The compound effect of vulnerability can be exaggerated due to further compounding; people who have four or more layers of vulnerability can be regarded as presenting *extreme vulnerability* to manipulation.

³⁸⁴ Mackenzie, Rogers and Dodds identify pathogenic vulnerabilities, which are “a subset of situational vulnerabilities that are particularly ethically troubling.” See Mackenzie et al., *supra* note 349 at 9. They discuss examples when a person is assigned a caretaker because of their vulnerability, and the caretaker abuses their role to exploit vulnerability. Relational vulnerability is not the same as pathogenic. Instead, it focuses on the authority and hierarchical relationships that may cause pathogenic consequences.

³⁸⁵ See also SAX, *supra* note 369, at 80.

³⁸⁶ See generally Esther Keymolen, *Trust In the Networked Era: When Phones Become Hotel Keys*, 22 TECHNÉ RES. PHIL. & TECH. 7 (2018).

³⁸⁷ See *Id.*

³⁸⁸ See Rogers, *supra* note 359, at 68–69.

³⁸⁹ Margaret Urban Walker, *Moral Vulnerability and the Task of Reparations*, in VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY (2013).

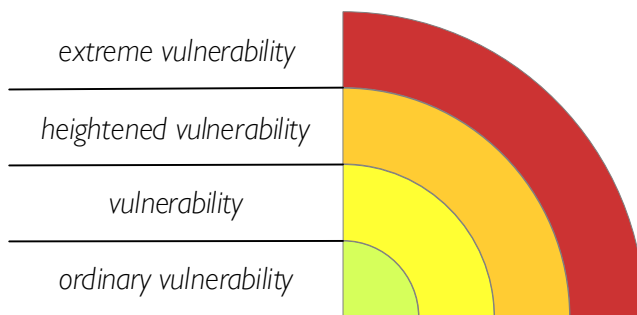


Figure 3:2. Levels of vulnerability (by author)³⁹⁰

Lastly, these levels of vulnerability can be used to evaluate how manipulative (and coercive) the practice is, which can be linked to the likelihood of an influence to exploit the vulnerability.³⁹¹ Section 3.3.3 uses the levels of vulnerability in Figure 3:2 to develop a framework that can evaluate the levels of manipulative practices and other forms of influence on a spectrum (Figure 3:3). Section 3.3.3 explains these levels by providing illustrative situations (*s1 – s7*) that exemplify the differences in levels and forms of influences. These situations are also placed in Figure 3:3.

3.3.3. The Spectrum of Influences

The likelihood of exploitation may depend on the specificity with which the influence is tailored to the target’s vulnerabilities.³⁹² In order for an influence to be considered manipulative under the definition of this thesis, the influence does not have to be intentionally targeted to these vulnerabilities. Instead, manipulative influence involves a deliberate attempt to influence a person, coupled with the agent’s expected awareness that the influence can exploit the target’s vulnerabilities.³⁹³ Therefore, how manipulative the practice is can depend on the target’s level of vulnerability.

³⁹⁰ The figure is a representation by the author of the “layered” concept of vulnerability developed in sections 3.3.1 and 3.3.2, where adding one layer of vulnerability increases the level of vulnerability by one on the spectrum.

³⁹¹ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 27.

³⁹² Susser, Roessler & Nissenbaum argue: “Indeed, targeting is best understood as an exacerbating condition: the more closely targeted a strategy is to the specific vulnerabilities of a particular manipulee, the more effective one can expect that strategy to be.” *Id.*

³⁹³ Klenk defends this point of view. See generally Klenk, *supra* note 305. Klenk argues against Susser, Roessler & Nissenbaum’s manipulation as a “hiddenness” view. However, this thesis finds that carelessness and hiddenness conditions are not self-excluding; instead, the fact that influence itself can be overt, but the vulnerability exploited due to the manipulator’s negligence of other person’s exposure supports the hiddenness argument. Critics may argue that such failure can be in any social situation or advertisement. However, when an agent of influence takes steps to turn up the notch of specificity with which they are to target a person’s characteristics to influence them – they also increase the likelihood that they will exploit the vulnerabilities.

Generally, targeting vulnerabilities can also be employed as a method for overt forms of influence. Vito Corleone, Mafia don from the movie *The Godfather*, increases the likelihood of his *coercive* attempts being effective by placing the head of his target’s favorite horse into his bed.³⁹⁴ Mr. Keating, the English teacher from the movie *Dead Poets Society*, also increases the likelihood of his *persuasive* attempts being effective by showing his students the picture of the dead alumni to encourage them to live extraordinary lives.³⁹⁵ As long as the target can become conscious of their own vulnerability, an influence that is likely to exploit this vulnerability cannot be classified as manipulative. Figure 3:3 illustrates how the specificity of targeting, hiddenness, and the likelihood of exploitation of vulnerability interact with forms of influence.

hidden	manipulative s5	highly manipulative s6	extremely manipulative s7	extremely manipulative
	persuasive s1	highly persuasive s2	coercive s3	highly coercive s4
targets	ordinary vulnerability	vulnerability	heightened vulnerability	extreme vulnerability

Figure 3:3. Spectrum of influences with situations (by author)³⁹⁶

This section illustrates differences between forms of influence and their levels based on levels of vulnerability in seven situations (reflected in Figure 3:3 as *s1-s7*) in which agent *y* aims to get target *x* to drink.³⁹⁷ Suppose a situation 1 (*s1*), where *y* asks *x* if they are up for having a drink. This situation reveals a *persuasive* attempt – it is clear that *y* wants *x* to have a drink, where *x* is ordinarily vulnerable. Suppose situation 2 (*s2*), where *x* has disclosed to *y* that martini is their favorite drink, and *y* asks *x* if they are up for having martinis. This situation reveals another but more persuasive attempt that appeals to the personal preference of *x*. Personal preference

³⁹⁴ THE GODFATHER (Paramount Pictures, 1972).

³⁹⁵ DEAD POETS SOCIETY (Touchstone Pictures, 1990).

³⁹⁶ The figure was developed by the author to illustrate differences in forms and levels of influence based on the theory of vulnerability and manipulation developed in Chapter 3 of this thesis.

³⁹⁷ The situations described in this section are adaptations of the “martini example” introduced by Susser, Roessler, and Nissenbaum. See Susser, Roessler, and Nissenbaum, *supra* note 38, at 18.

for martinis acts as a layer of vulnerability for x , who has the second-order preference of not having a drink that day. This situation reveals an influence to be *very persuasive*, as x is more than ordinarily vulnerable. Suppose situation 3 ($s3$), where x has also disclosed that they want to stop drinking, and they cannot be anywhere near vodka martinis; y makes a fine glass of shaken vodka martini and puts it in front of x . This situation reveals an influence that is as *coercive* as it is overtly tailored to the target, which is *highly vulnerable* to such an influence.³⁹⁸ Suppose situation 4 ($s4$), where x discloses to y that it is the end of a particularly stressful workday and he could use a drink if he was not trying to quit – in response to which y parades a fine glass of shaken vodka martini in front of them. This situation reveals a *highly coercive* attempt that overtly tries to influence a target that is extremely vulnerable.

An influence is overt in all of these four situations ($s1 - s4$). x knows that y is aware of the extent of their vulnerability and is conscious of y 's objectives and the nature of the influence. Let us suppose situation 5 ($s5$), where x does not explicitly ask y to join him for a drink; instead, y appears to x , sipping on the drink in front of him. This situation reveals a *manipulative* attempt in which y 's intentions are hidden, and x , as the target of the influence, is ordinarily vulnerable to such hidden influence. Suppose situation 6 ($s6$), where y learned from z that x is a lover of martinis, and they are holding not any other drink but a martini when they approach x . In this situation, y 's influence is hidden, and tailored to x , who is more than ordinarily vulnerable. Such influence is *highly manipulative*. Lastly, suppose situation 7 ($s7$) where y knows that x associates drinking with jazz and turns the music on while starting to drink a martini in front of x . This situation reveals an attempt at the hidden influence that is tailored to target those extremely vulnerable to the tailored influence and, therefore, is an *extremely manipulative* practice.³⁹⁹

In sum, a layered understanding of vulnerability provides a way to understand the different levels at which the influence can be manipulative as well as coercive. In the end, this thesis understands the actions of the agent to be manipulative to the extent to which they can exploit the target's decision-making vulnerabilities, given that the agent intends to influence a target towards a particular outcome, and some aspect of the influence remains hidden. All influence that overtly exploits human vulnerabilities can be conceptualized as coercion.

3.4. Conclusion: Manipulation

Thus, this section offers an answer to the second sub-question of this thesis:

³⁹⁸ Some Georgians will regard this as coercive but morally justified.

³⁹⁹ Again, the concept of manipulation in this thesis is morally neutral. In some situations, a person may find it morally justified to manipulate their friend to have a drink, and, indeed, this can be a form of entertainment. Similarly seduction in romantic relationships can be highly manipulative, and a form of play.

SQ2: what is manipulation?

Manipulation is an agent's successful and intentional attempt to influence a target towards an outcome, where an essential aspect of the influence remains hidden from the target's awareness, and the agent is aware that the method of influence can exploit the target's decision-making vulnerabilities. Manipulation is a successful influence – the target has behaved like the agent wanted. Manipulation can happen through deception or pressure. Manipulation contrasts with other forms of influence, such as persuasion and coercion, in that it is *hidden*. It contrasts with persuasion in that it takes away the target's ability to exercise choice. It contrasts with coercion in that it maintains the illusion of choice – as individuals believe they are exercising choice.

The success of an agent's attempts to manipulate depends on the likelihood of the actions exploiting human decision-making vulnerabilities. An action of an agent can be said to be manipulative if (1) an agent intends to influence a target towards a particular outcome, (2) an essential aspect of the influence remains hidden, and (3) the method of influence is likely to exploit the target's vulnerability. The likelihood of exploitation can be mapped out on the different levels of the target's susceptibility to manipulative influence, that can be evaluated based on target's inherent, situational, or relational vulnerabilities. An action can be "manipulative" if it is tailored to a target who is ordinarily vulnerable to being manipulated by this action. Additional layers of vulnerability can make a target "more than ordinarily vulnerable" or with "heightened vulnerability", and tailoring action to such a target can be considered "highly manipulative" or "extremely manipulative", depending on the level of vulnerability.

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 manipulateness 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 Commission* (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 manipulateness 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 action 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, Roessler, and Nissenbaum 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 Information*, 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. COMM’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*.

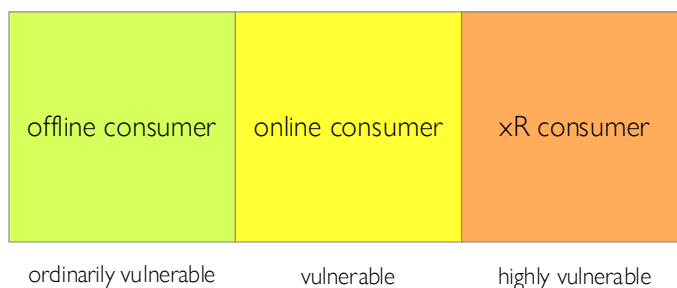


Figure 4:1. Levels of online consumer vulnerability (by author)⁴⁶⁴

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 manipulateness 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 definitions 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 (*MEPI: 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 disproportionately 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	<i>free-framing</i>	highly manipulative
MEP2	<i>the roach motel</i>	highly manipulative
MEP3	<i>obscure legalese</i>	highly manipulative
MEP4	<i>covert contracts</i>	highly manipulative
MEP5	<i>mastering</i>	highly manipulative

The adequate disclosure of otherwise hidden intentions can mitigate the manipulateness of these practices. Additional layers of vulnerability can increase the manipulateness 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	<i>covert content personalization</i>	highly manipulative
MEP7	<i>endless feed</i>	highly manipulative
MEP8	<i>auto-play</i>	highly manipulative
MEP9	<i>immersion preselection</i>	highly manipulative
MEP10	<i>social validation loop</i>	highly manipulative
MEP11	<i>gamification</i>	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)
<i>hidden tracking (MEP 12)</i> ⁵³⁶	A consumer is not presented with the notice about the data processing.	The processing of data is <i>hidden</i> 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 <i>must</i> choose to “see more” to reject (unequal pathways).	coercive
<i>inaccurate classification (MEP 13)</i> ⁵⁴⁰	The consumer is presented with “accept all” or “accept only essential cookies,” and data is inaccurately classified as <i>essential</i> .	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.

CONSUMER MANIPULATION VIA OBA

<i>confusing grounds</i> (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
<i>false hierarchy</i> (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
<i>misdirection</i> (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
<i>irrelevant third option</i> (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
<i>no withdraw button</i> 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 manipulateness 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	<i>hidden tracking</i>	extremely manipulative
MEP13	<i>inaccurate classification</i>	extremely manipulative
MEP14	<i>confusing grounds</i>	extremely manipulative
MEP15	<i>false hierarchy</i>	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	<i>misdirection</i>	highly manipulative
MEP17	<i>irrelevant third option</i>	highly manipulative
MEP18	<i>nagging</i>	highly manipulative
MEP19	<i>framing effects</i>	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, Kruijkemeier, 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	<i>hidden advertorials</i>	highly manipulative
MAP2	<i>hidden paid ranking</i>	highly manipulative
MAP3	<i>hidden ad personalization</i>	highly manipulative
MAP4	<i>hidden personalization criteria</i>	highly manipulative
MAP5	<i>hidden advertisers</i>	highly manipulative
MAP6	<i>hidden infrastructure</i>	highly manipulative
MAP7	<i>hidden data sharing</i>	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. COMMUN. 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

<u>MAP10: hardship targeting</u>	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

<i>MAP12: identity targeting</i>	<i>examples of categorizing identities</i>
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	<i>OCEAN targeting</i>	extremely manipulative
MAP9	<i>affect targeting</i>	extremely manipulative
MAP10	<i>hardship targeting</i>	extremely manipulative
MAP11	<i>persuasion profiling</i>	extremely manipulative
MAP12	<i>identity targeting</i>	extremely manipulative
MAP13	<i>sniper ad targeting</i>	extremely manipulative
MAP14	<i>lookalike audiences</i>	extremely manipulative
MAP15	<i>targeting minors</i>	extremely manipulative
MAP16	<i>targeting elderly</i>	extremely manipulative
MAP17	<i>targeting intellectual disabilities</i>	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.

CONSUMER MANIPULATION VIA OBA

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

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

CHAPTER 5. CONSUMER MANIPULATION HARMS OF 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 a coherent theory. With this in mind, this chapter answers the fourth sub-question of this thesis:

SQ4: what are the *harms* of consumer manipulation via online behavioral advertising?

In order to answer it, this chapter is divided into three parts: section 5.1. deliberates on traditional (market-based and rights-based) and new (capabilities-based) politically liberal theoretical approaches to conceptualizing consumer manipulation harms of OBA. Section 5.2. provides a typology of harm. Section 5.3 concludes the chapter by formulating the answer to the SQ4.

5.1. Theories of Harm

5.1.1. Consumer Manipulation Harms

This thesis understands consumer manipulation via OBA to be morally neutral and describes it as a successful attempt to hiddenly influence consumers by means of OBA.⁶²⁰ Manipulating a consumer can be considered “morally wrong” for various reasons (and degrees) depending on the normative lens through which it is evaluated.⁶²¹ For example, *deontologists* may regard consumer manipulation as wrong because it violates a categorical rule that humans should be treated “not merely as a means but also always as an end” (object formula).⁶²² In contrast, *consequentialists* may require an evaluation of consequences, such as economic, psychological, or physical implications, to determine the extent to which the phenomenon is wrongful.⁶²³

As a business-to-consumer commercial phenomenon, consumer manipulation via OBA has effects beyond moral considerations and is also legally relevant.⁶²⁴ Accordingly, this thesis refers to legally relevant adverse effects as *harms*.⁶²⁵ The Trans-Atlantic legal frameworks currently governing commercial relationships are typically based on the theories of harms conceptualized in response to the Industrial Revolution.⁶²⁶ There is an increasing consensus in academia that the theories underlying these legal frameworks cannot adequately capture the harms of the

⁶²⁰ See about “moralized” and “non-moralized” concepts of manipulation Wood, *supra* note 272 at 19–21.

⁶²¹ See “Autonomy, Dignity and Welfare” in SUNSTEIN, *supra* note 271 at 84–87.

⁶²² “Object formula,” also known as “humanity formula,” is one of four formulations of the categorical imperative. See IMMANUEL KANT, *GROUNDWORK FOR THE METAPHYSICS OF MORALS* 42 (2019). (“Act in such a way that you treat humanity whether in your own person or anyone else’s, never merely as a means, but also always as an end.”)

⁶²³ See Noggle, *supra* note 265 at 3.1. For example, consequentialists may morally justify manipulation for helping a person quit smoking, tolerate it for playfully seducing a lover, and condemn it for selling running shoes.

⁶²⁴ Some morally wrong practices are not relevant to the law. For example, while lying to one’s parents violates a tenet of Christian morality, it is not legally relevant in most cases. Moreover, legally relevant does not mean “illegal.” Some legally relevant adverse effects can be justified (self-defense) or excused (necessity). Lastly, an action may have legally relevant adverse effects but be morally justified. For example, a person seeking revenge may morally justify their actions based on the “eye for an eye” principle but cause legally relevant adverse effects.

⁶²⁵ In US context, *harms*, especially “legally cognizable harms” are referred to as the adverse effects that can be recognized by courts, and are closely linked with the “injury-in-fact” and “standing” (*locus standi*) doctrines. See Ido Kilovaty, *Legally Cognizable Manipulation*, 34 *BERKELEY TECH. L. J.* 449 (2019). See also Daniel Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 *BOSTON UNIV. L. REV.* 798 (2022). Reference to “harm” is inconsistent in the EU policy, also, because there is no overarching European private law legislation.

⁶²⁶ “Trans-Atlantic” here refers to the geographic area of the European and North American continents. See COHEN, *supra* note 28 at 143–151. See also Elettra Bietti, *A Genealogy of Digital Platform Regulation*, 7 *GEO. L. TECH. REV.* 39 (2021).

Information Age.⁶²⁷ Moreover, without an adequate theory of harm, policymakers struggle to evaluate the stakes at play when considering governing OBA, which has generated unprecedented wealth for providers of platforms.⁶²⁸ Similarly, without such a theory of harm, regulatory enforcement bodies may struggle to allocate their resources efficiently, and judges may fail to recognize the true interests at stake.⁶²⁹

Some skeptics dismiss the harmfulness of consumer manipulation via OBA because they do not see anything new compared to traditional persuasive advertising or that broad conceptualization of harm may disproportionately limit entrepreneurial freedom.⁶³⁰ Legal academia has responded to general skepticism by developing in-depth analyses of the Information Age’s adverse effects, focusing on privacy and data breach harms.⁶³¹ However, such a vantage point cannot wholly capture the heart of the matter regarding consumer manipulation.⁶³² This thesis broadens the analysis by focusing on consumer manipulation harms of OBA or legally relevant adverse effects of consumer manipulation via OBA.

Evaluating the harmfulness of consumer manipulation via OBA requires adopting a normative stance. Accordingly, this thesis scopes the discussion within theories of political liberalism that provide a theoretical basis for the legal

⁶²⁷ See COHEN, *supra* note 28 at 143–151. See also Citron and Solove, *supra* note 625. See also Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131, 2011 (2011).

⁶²⁸ Primary beneficiaries of OBA are providers of digital platforms such as Alphabet and Meta (section 2.3.3). It has become increasingly doubtful that advertisers and publishers engaged in OBA also benefit from this practice. Moreover, consumers find the services of online platforms valuable, and they can access the internet for free. See European Commission Study Recent Digital Advertising Developments, *supra* note 36. See also Citron and Solove, *supra* note 625 at 826–829.

⁶²⁹ For example, a lot of focus of regulatory enforcers has been given to the cookie banner dark patterns, but not to the core practice of OBA directly (section 4.2.3) See about this effect in ambiguity about harms in Citron and Solove, *supra* note 625 at 813. Note that Citron’s and Solove’s argument is more relevant in US adjudication. Domestic courts and CJEU increasingly adopt a broader view on harms in the Information Age. (section 6.1.3).

⁶³⁰ See Calo, *supra* note 38 at 1018–1034. Note that the “there is nothing new” argument suggests that OBA, similar to most traditional advertising, does not cross the threshold between persuasion and manipulation. In essence, Chapter 4 illustrated how this argument is wrong.

⁶³¹ See COHEN, *supra* note 28 at 143–151. See Ido Kirovaty, *Psychological Data Breach Harms*, 23 N. C. J. L. & TECH. 1 (2021). See also Citron and Solove, *supra* note 625. See also Calo, *supra* note 627. See also Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, (2016), <https://papers.ssrn.com/abstract=2885638> (last visited Mar 15, 2023). See also Daniel J. Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, 118 NORTHWESTERN UNIV. L. REV. 1 (2024).

⁶³² Sax takes a similar stance in the context of health-apps. See M. Sax, *Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps* 22 (2021). (“I want to focus on the potential of digital choice architectures to – often subtly – manipulate our behavior. If we frame this problematic in terms of privacy, we would fail to get to the heart of the problem. To be sure, the problem of privacy in the digital society is important in this context, but it is only a secondary problem.”)

frameworks in the EU.⁶³³ While there have been attempts in US academia to create a “theory of justice” that could act as the overarching theory for politically liberal countries in the Trans-Atlantic region, global post-World War II theories are typically polarized by two different sets of goals: advancing the free market (classical liberalism) and promoting human flourishing through human rights and democratic rule (liberal constitutionalism).⁶³⁴ Similarly, Information Age harms are typically evaluated from two perspectives roughly labeled as *market-based* and *rights-based* approaches.⁶³⁵ Both of these converge in that the central issue of consumer manipulation via OBA and the source of harm stem from undermining *personal autonomy* – people’s capability to make their own decisions.⁶³⁶ This thesis understands personal autonomy not as the capability of rational or ideal choosers but as that of ordinary human beings with cognitive biases, beliefs, desires, and

⁶³³ See “four branches of liberalism” in Bietti, *supra* note 626 at 8–10. Moreover, there are theoretical stances such as *communitarianism* that criticize liberal political philosophy to be overly concerned about the individual. See Daniel Bell, *Communitarianism*, in THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta & Uri Nodelman eds., Fall 2022 ed. 2022), <https://plato.stanford.edu/archives/fall2022/entries/communitarianism/> (last visited Mar 24, 2023). Nevertheless, these views hold only peripheral importance in public and private law. With this in mind, this thesis focuses primarily on *liberal* theories.

⁶³⁴ Most notable is Rawl’s *Theory of Justice*. See JOHN RAWLS, A THEORY OF JUSTICE: ORIGINAL EDITION (1971). See Bietti, *supra* note 626 at 8.

⁶³⁵ This thesis labels the approaches “market-based” and “rights-based” to disambiguate perspectives that are at times labeled in misleading ways. For example, US legal academics sometimes distinguish between “harm-based” and “rights-based” approaches. See Citron and Solove, *supra* note 625 at 809. This may wrongfully suggest that adverse effects on human rights are not harms. Sometimes, the market-based approach is framed as a “welfare” perspective. See Zarsky, *supra* note 38 at 172. See also SUNSTEIN, *supra* note 271 at 84. Reference here is to “welfare economics” and broader (*pure*) *welfarist* moral theory that is a specific form of *utilitarianism*. While utilitarianism measures the quality of life in any given society at total (or average) “utility”, satisfaction of preferences, welfarism acknowledges that preferences may be deformed, setting a goal of satisfying “authentic” preferences. See MARTHA C. NUSSBAUM, CREATING CAPABILITIES: THE HUMAN DEVELOPMENT APPROACH 81 (2011). The reference to welfare in online manipulation literature reflects the practice of measuring welfare (satisfaction of authentic preferences) in economic terms. In Europe, “welfare” is also widely used in slightly different contexts of welfare state, social welfare, and welfare benefits. Therefore, this thesis refers to market-based harms. As for rights-based harms, scholars have previously differentiated “autonomy-based” and “dignity-based” approaches, where autonomy refers to personal autonomy as defined in this thesis, and dignity to human entitlement not to be experimented upon or not to be treated as objects. See SUNSTEIN, *supra* note 271 at 96. See also Zarsky, *supra* note 38 at 20. In the European context, such formulation is unnecessary. In European legal doctrine, “dignity” has a more nuanced meaning than the mere prohibition of experimentation and covers autonomy interests.

⁶³⁶ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 35. Personal autonomy is not the same as “freedom.” See BEATE ROESSLER, THE VALUE OF PRIVACY 49 (2005). (“One must be free to be able to be autonomous, but not every free action is an autonomous one, and we expect people to choose, act, behave and live not only ‘freely’ but also autonomously”.) Further, freedom, can be understood as *non-interference* and *non-domination*. For freedom as non-interference see *Id.* at 44–49. For freedom as non-domination see PHILIP PETTIT, REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT (2002). Moreover, personal autonomy is not the same as moral autonomy, which refers to autonomy as a moral principle, for example, prescribed by the Kantian formulation of the categorical imperative. See KANT, *supra* note 622 at 65.

emotions vulnerable to influence.⁶³⁷ Berlin’s quote captures the essence of personal autonomy in an aspirational frame:

I wish my life and decisions to depend on myself, not on external forces. I wish to be the instrument of my own, not other men’s acts of will. I wish to be a subject, not an object [...] I wish to be somebody, not nobody [...] deciding, not being decided for [...] as if I were a thing [...] incapable of conceiving goals and policies of my own and realizing them.⁶³⁸

Understood this way, personal autonomy has conditions of *authenticity* and *capability*.⁶³⁹ Making autonomous decisions means making decisions one considers their own (authenticity).⁶⁴⁰ Making autonomous decisions requires the ability to discern such authentic reasons (capability).⁶⁴¹ Consumer manipulation undermines personal autonomy by making consumers incapable of deliberating on hidden influences that exploit their vulnerabilities, leading to decisions they cannot authentically regard as their own.⁶⁴²

Market-based and rights-based approaches take contrasting views on *why* undermining personal autonomy is harmful and to *what extent*. Both perspectives have limitations in conceptualizing Information Age harms. Sub-sections 5.1.2 and 5.1.3. evaluate consumer manipulation harms of OBA with market-based and rights-based approaches, respectively, and analyze their limitations. Sub-section 5.1.4 proposes a new method for examining consumer manipulation harms of OBA that combines market-based and rights-based approaches and works around their limitations.

5.1.2. Welfare: Free Market Approach

A free-market economy provides one approach to evaluate consumer manipulation harms. This approach reflects the utilitarian, classical liberalist

⁶³⁷ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 36.

⁶³⁸ Isaiah Berlin, *Four Essays On Liberty*, in TWO CONCEPTS OF LIBERTY 118 (1969).

⁶³⁹ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 36. Susser, Roessler, and Nissenbaum distinguish between “authenticity” and “competence.” This thesis ascribes to the substance of these conditions. However, it terms “competence” conditions as “capability” similar to Berlin’s definition of autonomy. See Berlin, *supra* note 638. The reader may notice closeness of such framing to Capability Approach later introduced in the thesis (*section 5.1.4*). Such framing is appealing for coherence of this thesis, but also for accuracy. *Capability* is ability to do something, and *competence* ability to do something well.

⁶⁴⁰ See Susser, Roessler, and Nissenbaum, *supra* note 38 at 36. (“And autonomous persons can (at least in principle) critically reflect on their values, desires, and goals, and act for their *own* reasons—i.e., endorse them *authentically* as their own.”)

⁶⁴¹ See *Id.* (“Autonomous persons have the cognitive, psychological, social, and emotional *competencies* to deliberate, to form intentions, and to act on the basis of that process.”)

⁶⁴² See on how online manipulation undermines two conditions of autonomy in *Id.* at 38.

perspective that sets the *utility* or satisfaction of people’s preferences as the ultimate societal goal and prescribes a free economic exchange – the *market* – to create a social order that efficiently maximizes it.⁶⁴³ Welfare economics considers the free market as a mechanism to maximize social well-being or *welfare* by supplying products and services that satisfy people’s authentic preferences. Nevertheless, the welfarist point of view is premised on the perception that people’s authentic preferences can only be known to them, and therefore, their authentic or autonomous choice in the market is what ensures maximizing welfare.⁶⁴⁴ Free market economists suggest that in the absence of government intervention, the market can achieve “Pareto efficiency,” a situation in which no individual can benefit more without harming another.⁶⁴⁵ This equilibrium of a free and perfectly competitive market is premised on maximizing utility, or well-being, which economists refer to as *welfare*.⁶⁴⁶

The free market theorists see the role of the government as intervening in the market only to prevent harm from occurring between private parties (“harm principle”).⁶⁴⁷ In business-to-consumer relationships, such harm is typically theorized as a reduction in consumer welfare, which refers to the utility or well-

⁶⁴³ The foundations of the classical liberalist view on the market economy are typically located in Adam Smith’s *Wealth of Nations*. Smith believed that individuals pursuing their “enlightened” self-interest would compete in the marketplace and be led by the “invisible hand” of the market to maximize societal well-being. See SMITH, *supra* note 317. See also JOHN STUART MILL, ON LIBERTY 142 (2nd ed. ed. 1859). See also about market-based harms of online manipulation in Zarsky, *supra* note 38 at 172. See market-based approach to manipulation harms in SUNSTEIN, *supra* note 271 at 85.

⁶⁴⁴ Such a view on satisfaction of preferences can, particularly, be attributed to Mill and Hayek. See MILL, *supra* note 643 at 16. (“People decide according to their preferences.”) See also FRIEDRICH A. HAYEK, THE MARKET AND OTHER ORDERS 384 (Bruce Caldwell ed., 2013). (“[T]he awareness of our irremediable ignorance of most of what is known to somebody [who is a planner] is the chief basis of the argument for liberty.”) See also NUSSBAUM, *supra* note 635 at 93.

⁶⁴⁵ Pareto efficiency is named after Italian economist Vilfredo Pareto who first developed the theory. Moreover, there can be three different types of efficiency. *Allocative efficiency* refers to a situation when market price equals marginal cost, and everyone willing and able to buy a product will do so. *Productive efficiency* refers to a competitive market with the lowest possible production costs, lowering prices. Lastly, *dynamic efficiency* concerns how the market delivers innovation and technological progress. See ALISON JONES & BRENDA SUFRIN, EU COMPETITION LAW: TEXT, CASES, AND MATERIALS 8–11 (Fourth ed. 2011).

⁶⁴⁶ “Welfare” is the term that *economists* refer to denote overall physical, mental, emotional, and financial well-being, but is mostly measured in economic value. “Welfare economics” is a branch of economics that studies economic activities with their benefit in society. See *Id.* at 4.

⁶⁴⁷ “Harm principle” is famously articulated by MILL, *supra* note 643 at 18. (“That the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others.”) See about harms in private law Duncan Kennedy, *A Transnational Genealogy of Proportionality in Private Law*, in THE FOUNDATIONS OF EUROPEAN PRIVATE LAW (Roger Brownsword et al. eds., 2011). See also Benedicte Fauvarque-Cosson, *The Need for Codified Guiding Principles and Model Rules in European Contract Law*, in THE FOUNDATIONS OF EUROPEAN PRIVATE LAW (Roger Brownsword et al. eds., 2011).

being consumers derive from consuming goods and services.⁶⁴⁸ Consumer welfare can be reduced either through “personal detriment” to the consumer or through “structural detriment” on the market that negatively affects the consumer’s interests.⁶⁴⁹ While personal detriment affects a consumer in a specific transaction (e.g., buying a damaged product that causes physical harm), structural detriment arises due to inefficiencies in the market (e.g., products are overpriced due to lack of competition).⁶⁵⁰ Perspectives of personal and structural detriment lead to different conclusions, not only as to whether it is directed at an individual consumer or market as a whole but also what counts as a harmful outcome.⁶⁵¹ Similarly, consumer manipulation harms of OBA can be categorized in two forms.

First, particular business practices, such as a single dark pattern or a manipulative advertisement, can be personally detrimental to the consumer from the market perspective if they lead to direct financial loss, loss of time, and psychological or physical injury.⁶⁵² Such a market perspective is consequentialist – undermining personal autonomy becomes detrimental when consumer manipulation affects other interests (e.g., physical health and economic interests).⁶⁵³ Moreover, such adverse effects reduce consumer welfare and, therefore, are considered harmful if they outweigh the benefits to the consumer.⁶⁵⁴ Even though the market approach includes non-financial detriments, cost-benefit analyses are typically monetary and, therefore, require translation of non-tangible detriment into an economic quantity that acts as a proxy for well-being.⁶⁵⁵

Second, businesses can also harm consumers by causing structural detriment or causing the market to fail, leading to inefficient market outcomes (“market failure”).⁶⁵⁶ Market failure harms are primarily ascribed to the erosion of competition when private parties transform their economic freedom into enough

⁶⁴⁸ See JONES AND SUFRIN, *supra* note 645 at 8–11. Consumer welfare is often identified with the economic concept of “consumer surplus” that is difference between the price they are willing to pay for a good or service and actual price they pay. However, in this thesis consumer welfare refers to the broader concept of physical, mental and financial well-being.

⁶⁴⁹ See EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, *Study on Measuring Consumer Detriment in the European Union: Final Report, Part I: Main Report*, 24 (2017).

⁶⁵⁰ *Id.* at 26–27.

⁶⁵¹ *Id.* at 2.

⁶⁵² *Id.* at 38–40.

⁶⁵³ *Id.* at 38–40.

⁶⁵⁴ See Zarsky, *supra* note 38 at 172. See SUNSTEIN, *supra* note 271 at 85.

⁶⁵⁵ See Zarsky, *supra* note 38 at 172. See SUNSTEIN, *supra* note 271 at 85. See also NUSSBAUM, *supra* note 635 at 81.

⁶⁵⁶ See ROBERT BALDWIN & MARTIJN CAVE, UNDERSTANDING REGULATION: THEORY STRATEGY, AND PRACTICE 15–22 (2nd ed. 2012).

power to distort competition and cause inefficiencies in the market.⁶⁵⁷ Market failures can also occur due to other factors, such as negative externalities.⁶⁵⁸ For example, a business may maintain competitive prices by polluting, causing indirect harm to the consumer.⁶⁵⁹ Such market failures can decrease consumer welfare and cause harm by reducing consumers' trust in the market, reducing innovation, reducing quality, and increasing prices for goods and services.

Regarding structural detriment, there is an alternative way to measure harm – the *total welfare* standard considers not only the benefits that accrue to consumers but also the costs and benefits of other affected parties, including businesses.⁶⁶⁰ As the market capitalization of platforms that rely on OBA has reached \$4 trillion, the choice between total welfare and consumer welfare standards may be relevant to evaluating OBA's consumer manipulation harms.⁶⁶¹ The European Commission has continuously affirmed consumer welfare as the objective of the EU competition policy and a standard to evaluate harms within the EU markets.⁶⁶²

Around the globe, but particularly within the EU, industrial policies have expanded the notion of welfare to include a variety of social goals.⁶⁶³ According to the Lisbon Treaty, one of the goals of the EU is to establish a “highly competitive social market economy.”⁶⁶⁴ The reference to the “social market” is typically interpreted as capturing non-economic social interests of the community, such as sustainability or diversity, as societal values.⁶⁶⁵ The EU's approach to a free market economy with emphasis on social and political values is sometimes “Rhine capitalism,” getting its name from the river Rhine that runs through Germany, France, and Benelux countries associated with formulating such social value-driven

⁶⁵⁷ See JONES AND SUFRIN, *supra* note 645 at 4. See about role of law to protect market in SMITH, *supra* note 317 at 20–21.

⁶⁵⁸ There are other sources of market failures. For the overview see BALDWIN AND CAVE, *supra* note 656 at 15–22.

⁶⁵⁹ *Id.*

⁶⁶⁰ Svend Albæk, *Consumer Welfare in EU Competition Policy*, in AIMS AND VALUES IN COMPETITION LAW, 72 (Caroline Heide-Jørgensen et al. eds., 2013).

⁶⁶¹ Zingales and Lancieri, *supra* note 12 at 6. See also Largest Companies by Market Cap, *supra* note 13.

⁶⁶² MARIO MONTI, *The Future for Competition Policy in the European Union* (2001), https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_01_340/SPEECH_01_340_EN.pdf. (“[T]he goal of competition policy, in all aspects, is to protect consumer welfare by maintaining a high degree of competition in the common market. Competition should lead to lower prices, wider choice of goods, and technological innovation.”) See about objectives of the EU consumer policy JONES AND SUFRIN, *supra* note 645 at 44–46.

⁶⁶³ See JONES AND SUFRIN, *supra* note 645 at 51.

⁶⁶⁴ Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306), art. 3.

⁶⁶⁵ See JONES AND SUFRIN, *supra* note 645 at 41. See about “interests” and “values” On Interests and Values, MAASTRICHT UNIVERSITY LAW BLOG (Sep. 6, 2019), <https://www.maastrichtuniversity.nl/blog/2019/09/interests-and-values> (last visited Jul 3, 2023).

economic policies.⁶⁶⁶ Rhine capitalism is often contrasted with the Anglo-Saxon approach to the market economy, referred to as “neo-liberalism”, which sees meeting non-economic social interests merely as a consequence of economic freedom and an unhindered market.⁶⁶⁷

Typically, integrating social values within the goals of the market is criticized as a tool for safeguarding these values and evaluating societal harms for at least two reasons. On the one hand, economists criticize using competition policies for objectives other than achieving efficiency.⁶⁶⁸ On the other hand, legal theorists criticize such an approach because it requires a cost-benefit analysis and applying monetary value as a proxy for societal values, such as personal autonomy, that they regard as not quantifiable.⁶⁶⁹ An approach based on human rights is typically proposed as an alternative solution to capturing the harms to societal values.⁶⁷⁰ Section 5.1.3 elaborates on such a human rights approach in the context of the harms of consumer manipulation via OBA.

5.1.3. Dignity: Human Rights Approach

The rights-based, *liberal constitutionalist* approach to harm evaluates the effects of consumer manipulation on the interests protected by the framework of human rights.⁶⁷¹ The United Nations (UN) has defined the list of such values that states are expected to respect, protect, and promote across the globe.⁶⁷² In general, theories of human rights have transformed from protecting the interests of individual human beings from state power (“non-interference”) to guiding the policy with the

⁶⁶⁶ See JONES AND SUFRIN, *supra* note 645 at 41. “Ordoliberalism” is also social market economy model from Freiburg School (Germany) in contrast to “neoliberalism” of the Chicago School (US). While the EU policy was largely inspired by ordoliberal and rhine model capitalism, eventually neo-liberal models have had significant impact on the EU policy. See generally Kati J., Cseres, *EU Competition Law and Democracy in the Shadow of Rule of Law Backsliding*, in THE EVOLVING GOVERNANCE OF EU COMPETITION LAW IN A TIME OF DISRUPTIONS: A CONSTITUTIONAL PERSPECTIVE (C. Colombo & M. Eliantonio, K. Wright, eds.).

⁶⁶⁷ See Bietti, *supra* note 626 at 36–38.

⁶⁶⁸ See JONES AND SUFRIN, *supra* note 645 at 51.

⁶⁶⁹ See generally Tony Prosser, *Regulation and Social Solidarity*, 33 J. L. & Soc. 364 (2006).

⁶⁷⁰ See BALDWIN AND CAVE, *supra* note 656 at 15–22. 22-23.

⁶⁷¹ See for theoretical overview of rights-based perspective in relation to permissible harm Susanne Burri, *A Rights-Based Perspective on Permissible Harm*, Feb. 14, 2015, <http://etheses.lse.ac.uk/1060/> (last visited Apr 4, 2023).

⁶⁷² The foundational body of UN international human rights law is often referred to as International Bill of Human Rights (IBHR), that is formed by G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948). [hereinafter UDHR] as well as the *Twin Covenants*: G.A. Res. 2200(XXI) A, International Covenant on Civil and Political Rights (Dec. 16, 1966). [hereinafter ICCPR] and G.A. Res. 2200(XXI) A, International Covenant on Economic, Social and Cultural Rights (Dec. 16, 1966). [hereinafter ICESCR]. IBHR reflects normative framework of “respect” (negative vertical), “protect” (negative horizontal), and “fulfill” (positive). See Polly Vizard, Sakiko Fukuda-Parr & Diane Elson, *Introduction: The Capability Approach and Human Rights*, 12 J. HUM. DEV. CAPAB. 1, 4 (2011).

objective of human flourishing.⁶⁷³ This transformation is most vivid in the constitutionalism of the EU, which places human rights at the forefront of EU policy (parallel to economic power, as described in the section).⁶⁷⁴ The EU human rights framework is formed by the Charter for the Fundamental Rights of the European Union (CFREU) and the European Convention on Human Rights (ECHR).⁶⁷⁵ This framework is grounded in the concept of *human dignity*, which is often affirmed as the “essence” of the human rights framework in the EU or the *value* at the core of the interests this framework protects.⁶⁷⁶

In EU constitutionalism, human dignity can be best understood as a restatement of the deontological *humanity formula* that a human being must never be treated “merely as a means but also always as an end”.⁶⁷⁷ The European Commission has often explained this concept to be a form of the basic norm (or *Grundnorm*) from which all other norms derive their validity:

Human dignity is the basis of all fundamental rights. It guarantees the protection of a person from being treated as a mere object by the State or by its fellow citizens.⁶⁷⁸

⁶⁷³ See Vizard, Fukuda-Parr, and Elson, *supra* note 672 at 6.

⁶⁷⁴ See for the EU rights-based constitutionalism CATHERINE DUPR, *THE AGE OF DIGNITY: HUMAN RIGHTS AND CONSTITUTIONALISM IN EUROPE* (1st ed. ed. 2015). See for such transformation in the context of the digital age DE GREGORIO, *supra* note 154.

⁶⁷⁵ CFREU, *supra* note 43. ECHR, *supra* note 44. CRFEU and ECHR are complementary – CRFEU explicitly connects itself with the ECHR.

⁶⁷⁶ For example, *Vinter v. UK*, European Court of Human Rights (ECtHR) was considering whether a life sentence without the possibility (hope) of release was inhuman or degrading treatment. *Vinter and Others v. the United Kingdom* [GC], nos. 66069/09, 130/10 and 3896/10, ECHR 2013. (“Similar considerations must apply under the Convention system the *very essence* of which, as the Court has often stated, is respect for human dignity”) [emphasis added] See *generally* DUPR, *supra* note 674. Note that, *Vinter v. UK* also reflects the influence of West German constitutionalism on the ECtHR, as explicitly refers to their interpretation of human dignity in the judgment. Human dignity is also the first foundational value referred to in Lisbon Treaty. See Treaty of Lisbon, *supra* note 664 art. 2. (“The Union is founded on the values of respect for human dignity, freedom, democracy, equality, rule of law, and respect for human rights, including the rights of persons belonging to minorities.”) Moreover, human dignity is a centerpiece of the CFREU. Article 1 (“Human Dignity”) of TITLE 1 (“DIGNITY”) reads: “Human dignity is inviolable. It must be respected and protected.” Moreover, the preamble explains: “Conscious of its spiritual and moral heritage, the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity”. See CFREU, *supra* note 43.

⁶⁷⁷ EUROPEAN COMMISSION, *2010 Annual Report from the Commission on the Application of the EU Charter of Fundamental Rights*, (2010). Human dignity is notoriously difficult concept to understand, and define, and is often an object of skepticism and criticism. Some critics refer to it as “useless” or “empty”. However, these scholars miss an important aspect of human dignity – its exact meaning is not supposed to be known. Rather it provides a heuristic tool for the governance of change, where current societal values can be defended by reference to it. See DUPR, *supra* note 674 at 16.

⁶⁷⁸ EUROPEAN COMMISSION, *supra* note 677. For “Grundnorm” See Stephen Riley, *The Function of Dignity*, 5 AMST. L. FORUM, 103 (2013).

Ascribing to this concept, the highest possible normative value, above the sanctity of human life,⁶⁷⁹ reveals the EU constitutionalism and human rights to be a form of *humanism* – while it acknowledges that human beings can be citizens, workers, patients, or consumers, it commits of always also viewing them as humans.⁶⁸⁰ Grounding rights in human dignity is a reminder of the total annihilation of humanity during World War II and a commitment to “never again” permitting such inhumanity that is always possible.⁶⁸¹ Therefore, human dignity functions as a problem-solving tool.⁶⁸² It places the source of a comprehensive set of human rights in people’s humanity, ensuring the protection of the interests of the most vulnerable.⁶⁸³ It also establishes boundaries that are never permissible to cross.⁶⁸⁴

Title I of the CFREU formulates these boundaries as the right not to be arbitrarily killed (Article 2 CFREU),⁶⁸⁵ not to have physical and mental integrity breached (Article 3 CFREU),⁶⁸⁶ not to be tortured or subjected to inhuman and degrading treatment (Article 4 CFREU),⁶⁸⁷ and not to be subjected to slavery or trafficking (Article 5 CFREU).⁶⁸⁸ These rights, referred to together as “dignity rights”, reveal the very minimum of people’s quality of life necessary for life in dignity.⁶⁸⁹ Moreover, these rights must be respected so that other rights, such as

⁶⁷⁹ This suggests that human beings cannot be reduced to mere biological existence or “bare life”. See DUPR, *supra* note 674 at 174.

⁶⁸⁰ *Id.* at 172–182.

⁶⁸¹ *Id.* at 28–29. Furthermore, it inverts the relationship between the state and the individual – affirming the latter’s humanity and personal autonomy as the source and the boundaries of political power. *Id.* at 36.

⁶⁸² DUPR, *supra* note 674 at 16–23, 58–61.

⁶⁸³ See generally Mary Neal, *Not Gods but Animals: Human Dignity and Vulnerable Subjecthood*, 23 LIVERP. L. REV. 177 (2012). See also DUPR, *supra* note 674 at 175.

⁶⁸⁴ DUPR, *supra* note 674 at 174.

⁶⁸⁵ Article 2: 1. “Everyone has the right to life.” 2. “No one shall be condemned to the death penalty, nor executed.” CFREU, *supra* note 43, art. 2.

⁶⁸⁶ Article 3: 1. “Everyone has the right to respect for his or her physical and mental integrity.” 2. “In the fields of medicine and biology, the following must be respected in particular: (a) the free and informed consent of the person concerned, according to the procedures laid down by law; (b) the prohibition of eugenic practices, in particular those aiming at the selection of persons;” (c) the prohibition on making the human body and its parts as such a source of financial gain; (d) the prohibition of the reproductive cloning of human beings.” CFREU, *supra* note 43, Article 3.

⁶⁸⁷ Article 4: “No one shall be subjected to torture or to inhuman or degrading treatment or punishment.” CFREU, *supra* note 43, art. 3.

⁶⁸⁸ Article 5: 1. “No one shall be held in slavery or servitude.” 2. “No one shall be required to perform forced or compulsory labour.” 3. “Trafficking in human beings is prohibited.” CFREU, *supra* note 43, art. 5.

⁶⁸⁹ See also Lexo Zardiashvili & Eduard Fosch-Villaronga, “*Oh, Dignity Too?*” *Said the Robot: Human Dignity as the Basis for the Governance of Robotics*, 30 MINDS & MACH. 121 (2020). See DUPR, *supra* note 674 at 77.

privacy or freedom of expression, can be actualized.⁶⁹⁰ However, regarding dignity as the “essence” of other rights means that each right has a minimum core that cannot be crossed to ensure a quality of life worthy of dignity.⁶⁹¹ By establishing dignity as its minimum core, the fundamental human rights in the EU provide a theoretical framework for analyzing consumer manipulation harms of OBA. Whether or not consumer manipulation via OBA puts under pressure the core quality of life protected by “dignity rights” is evaluated in *section 5.2.7*.

OBA, which typically relies on personal data, comes in particularly strong tension with the EU theoretical framework of rights that, unlike other frameworks, includes the right to protection of personal data as a fundamental right.⁶⁹² In 1890, US legal scholars already articulated the impacts of technology on “the right to privacy” as the “right to be let alone.”⁶⁹³ The EU human rights framework recognizes such interest and captures it in the “right to private life and correspondence,” but it also goes beyond to safeguard people’s interest to be in control of personal information about them and formulates a separate “right to personal data protection.”⁶⁹⁴ This is primarily because privacy violations have led to unparalleled atrocities on the European continent. For example, the Nazi regime used data about religion processed by the Dutch government to wipe out the Jewish population in the Netherlands.⁶⁹⁵ The EU’s right to protect personal data is often called the right to “informational self-determination,”⁶⁹⁶ as it intends to uphold

⁶⁹⁰ See EUROPEAN COMMISSION, *supra* note 677. (“The rights and freedoms under the title Dignity, such as the right to life, and prohibition of torture and slavery, must be respected so we can exercise other rights and freedoms in the Charter, for example, freedom of expression and freedom of association.”)

⁶⁹¹ See DUPR, *supra* note 674 at 77. (“The phrase ‘life in dignity and independence’ is not defined, but arguably includes a core quality of life as protected by the Title I human dignity rights.”)

⁶⁹² See generally ZUIDERVEEN BORGESIU, *supra* note 25.

⁶⁹³ In the Harvard Law Review article, sometimes called “the most famous law review article” Warren and Brandeis formulated privacy as “right to be let alone” or solitude. See generally Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

⁶⁹⁴ Such privacy as control of personal information was formulated by ALAN WESTIN, *PRIVACY AND FREEDOM* (1967). (“The right of the individual to decide what information about himself should be communicated to others and under what circumstances”)

⁶⁹⁵ Due to availability of such data the Jewish population of the Netherlands had the lowest survival percentage (23%) among all European countries. See Marnix Croes, *The Holocaust in the Netherlands and the Rate of Jewish Survival*, 20 HOLOCAUST GENOCIDE STUD. 474 (2006).

⁶⁹⁶ “Informational self-determination” was formulated by the West German federal constitutional court in 1983 in the case relating to census. Bundesverfassungsgericht [BVerfG][Federal Constitutional Court] Dec. 15, 1983, (self-determination) 1 BvR 209/83, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983 (Ger.) translation at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. (“Restrictions of this right to ‘informational self-determination’ are only permissible if they serve an overriding public interest”)

personal autonomy, for example, by requiring an individual’s consent.⁶⁹⁷ Although it is ultimately grounded in human dignity, processing must be *fair* regardless of how the data is acquired.⁶⁹⁸

Tensions between OBA and the EU right to personal data protection have received much academic attention because this right emerged to specifically respond to the advance of information technologies and their appetite for personal data processing, and OBA can be seen as the culmination of using such technologies.⁶⁹⁹ However, the resulting myopic view on this tension fails to capture that personal data protection is one of many interests safeguarded by the EU rights framework under threat by consumer manipulation via OBA.⁷⁰⁰ Beyond rights of privacy and personal data protection, CFREU lists other *freedoms* in Title II, such as the right to liberty and security,⁷⁰¹ freedom of thought,⁷⁰² freedom of expression and information,⁷⁰³ freedom to conduct business,⁷⁰⁴ and right to property⁷⁰⁵ that can all come under pressure by consumer manipulation that in essence undermines personal autonomy.⁷⁰⁶

As consumer manipulation exploits human vulnerabilities that at times stem from unique differences of individuals, it may have adverse effects on the set of

⁶⁹⁷ Article 8: 1. “Everyone has the right to the protection of personal data concerning him or her.” 2. “Such data must be processed *fairly* for specified purposes and on the basis of the *consent* of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.” CFREU, *supra* note 43, art. 8.

⁶⁹⁸ CFREU, *supra* note 43, art. 8. *See* about grounding in human dignity BVerfG, 1 BvR 209/83, *supra* note 696. (“The value and dignity of the person, acting in free self-determination as a member of a free society, are at the centre of the Basic Law. In addition to the constitutional guarantees laid down in specific freedoms, the general right of personality, guaranteed in Art. 2(1) in conjunction with Art. 1(1) of the Basic Law, serves to protect these interests; this protection may gain even more significance in light of modern developments that pose new risks to one’s personality”)

⁶⁹⁹ First modern personal data protection law was introduced in 1970 in Hesse, Germany to respond to the advancements of computer technologies. In 1973, Sweden introduced first national data protection legislation called Data Act. In 1978 Germany introduced German Federal Data Protection Act. Data Privacy Act: A Brief History of Modern Data Privacy Laws, EPERI (2018), <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws> (last visited Apr 5, 2023).

⁷⁰⁰ *See e.g.* Leiser criticizes such a view on personal data protection (in the context of dark patterns), and calls for regulatory pluralism to also include protection of consumer interests. *See* Leiser, *supra* note 466.

⁷⁰¹ Article 6: “Everyone has the right to liberty and security of person”. *See* CFREU, *supra* note 43, art. 6.

⁷⁰² *Id.*, art. 10.

⁷⁰³ *Id.*, art. 11.

⁷⁰⁴ *Id.*, art. 16.

⁷⁰⁵ *Id.*, art. 17.

⁷⁰⁶ While Title II refers to “Freedoms”, its normative core is personal autonomy. Such an argument is further defended in the section about Capabilities Approach (*section 5.1.4*) How the interests protected by these rights come under pressure will be addressed in th *section 5.2*.

rights in Title III (*equality*) of the CFREU, such as non-discrimination,⁷⁰⁷ equality between women and men,⁷⁰⁸ the rights of the child,⁷⁰⁹ the rights of the elderly,⁷¹⁰ and persons with disabilities.⁷¹¹ The rights-based approach can also see adverse effects on social and economic rights listed in Title IV (*solidarity*) of CFREU, such as environmental protection,⁷¹² consumer protection,⁷¹³ and the right to access services of general economic interests.⁷¹⁴ Scholars often see OBA as instrumentalizing consumers by commodifying personal data and manipulating them, raising the question of to what extent this practice directly challenges the fundamental commitment to human dignity and the core quality of life that dignity rights aim to protect.⁷¹⁵ At first glance, the rights-based approach to consumer manipulation reveals a comprehensive picture of what is at stake by listing interests negatively affected by the practice. However, such an approach is characterized by at least four limitations.

Firstly, theories of human rights frameworks are typically judge-made – they are constructed through adjudication and legislative action and rarely achieve a level of coherence attributed to frameworks of normative ethics.⁷¹⁶ Even in the EU, where human rights adjudication has relatively solid normative foundations, different interpretations of *human dignity* can lead to different, at times opposing, outcomes regarding crucial social issues such as euthanasia or abortion.⁷¹⁷

Secondly, while the EU recognizes social and economic rights, they are rarely considered equally important as other interests.⁷¹⁸ Meanwhile, OBA is a market practice that has enabled the rise of businesses that are together valued at more than four trillion euros.⁷¹⁹ As these companies generate revenue through OBA, they have significant economic effects on consumers directly and indirectly by affecting advertisers and publishers.⁷²⁰ To fully understand the consumer manipulation harms

⁷⁰⁷ CFREU, *supra* note 43, art. 21.

⁷⁰⁸ *Id.*, art. 23.

⁷⁰⁹ *Id.*, art. 24.

⁷¹⁰ *Id.*, art. 25.

⁷¹¹ *Id.*, art. 26.

⁷¹² *Id.*, art. 37.

⁷¹³ *Id.*, art. 38.

⁷¹⁴ *Id.*, art. 36.

⁷¹⁵ See ZUBOFF, *supra* note 20.

⁷¹⁶ See generally Martha C. Nussbaum, *Capabilities and Human Rights*, 66 *FORDHAM L. REV.* (1997).

⁷¹⁷ See C. McCrudden, *Human Dignity and Judicial Interpretation of Human Rights*, 19 *EUR. J. INT. L.* 655, 692 (2008).

⁷¹⁸ See DUPR, *supra* note 674 at 108–110.

⁷¹⁹ See Zingales and Lancieri, *supra* note 12 at 6. See also *Largest Companies by Market Cap*, *supra* note 13.

⁷²⁰ See e.g., CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33. See also European Parliament Study Online Advertising & Consumer Choice, *supra* note 36.

of OBA, these economic effects must be integrated into the overarching framework for assessing its harms, which may be difficult via an exclusively rights-based approach.

Thirdly, the rights-based approach points to normatively powerful stakes, such as boundaries that human dignity commitment poses. While some scholars claim that consumer manipulation via OBA allows gatekeeper platforms to wield power to cross such fundamental commitments,⁷²¹ others are skeptical of the OBA industry amounting to the weight of tyrannical governments.⁷²² Human dignity commitment protects humanity against harms of the highest magnitude, such as torture, slavery, and arbitrary killing. Systematic manipulation of consumers may theoretically amount to crossing this boundary.⁷²³ However, arguing for or against such a view is extraordinarily controversial and most likely can only be resolved by a clear judicial stance.⁷²⁴ Without such evaluation, a rights-based framework does little to shed light on the boundaries of consumer manipulation without adopting an additional normative framework that fills these gaps.

Fourthly, a rights-based approach grounded in human dignity is often criticized because it focuses on the individual instead of the collective and society.⁷²⁵ Such a view is understandable – human dignity recognizes, respects, protects, and promotes humanity in each individual. However, it also acts as a constitutional tool that protects groups of individuals, such as children or consumers, and collective, societal values, such as democracy.⁷²⁶

In sum, human rights provide a comprehensive framework for evaluating consumer manipulation harms, but they also have certain limitations, such as prioritizing civil ahead of economic interests and lacking a coherent normative substance. With this in mind, section 5.1.4 attempts to synthesize market-based and human rights approaches to create a holistic framework that captures the consumer manipulation harms of OBA.

5.1.4. Unifying Strands: Capability Approach

Constitutional documents are primarily concerned with promoting people's well-being and protecting their fundamental rights by limiting state power so that

⁷²¹ See ZUBOFF, *supra* note 20. See also Blaire Rose, *The Commodification of Personal Data and The Road to Consumer Autonomy through the CCPA*, 15 (2021).

⁷²² See Calo, *supra* note 38 at 1031.

⁷²³ See about human dignity as the boundaries of capitalism in DUPR, *supra* note 674 at 108–110.

⁷²⁴ Richards was one of the first scholars to call for legal and social restrictions for the online businesses in the Age of Surveillance, and also highlighted the challenges to such rulemaking. See Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

⁷²⁵ G.A. van der Wal, *The Individualism of Human Rights*, 18 RECHTSFILOS. EN RECHTSTHEOR. 195 (1989).

⁷²⁶ See DUPR, *supra* note 674 at 66–70.

individuals can express their autonomy and live fulfilling lives.⁷²⁷ However, as the twenty-first century gave way to the rise of non-state power, modern “digital” constitutionalism is also concerned with applying fundamental rights horizontally to limit private power and establish a minimum standard of well-being while continuously creating a competitive market environment for increasing quality of life.⁷²⁸ The EU, particularly in digital markets, is concerned with balancing the free market and human rights goals.⁷²⁹ Traditional political theories, primarily focused on *fairness* in the allocation of resources, have not been able to create a synthesis between market and human rights perspectives in a way that adequately responds to the rise of “algorithmic” power.⁷³⁰ In the absence of a coherent normative framework, market, and human rights goals are sometimes seen as clashing.⁷³¹ As a result, the philosophical study of *ethics* has been increasingly informing the EU digital policy.⁷³²

The *capability approach* is a normative theory that can help synthesize market-based and rights-based perspectives for formulating consumer manipulation harms of OBA.⁷³³ One of the imperatives of the capability approach is the same as the free

⁷²⁷ See DE GREGORIO, *supra* note 154 at 3.

⁷²⁸ *Id.*

⁷²⁹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade, (2021), <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118> (last visited Apr 8, 2023). (“[O]ur stated ambition is more relevant than ever: to pursue digital policies that empower people and businesses to seize a human centred, sustainable and more prosperous digital future.”) See also EUROPEAN COMMISSION, *Shaping Europe’s Digital Future* (2020). (“A European way to digital transformation which enhances our democratic values, respects our fundamental rights, and contributes to a sustainable, climate-neutral and resource-efficient economy.”) See DE GREGORIO, *supra* note 154 at 31–32.

⁷³⁰ Rawl’s theory of political liberalism articulated in *A Theory of Justice* is the most influential political theory in twentieth century that attempts to synthesize market and rights based goals. See RAWLS, *supra* note 634. However, Rawls’s theory has a strong emphasis on fairness in resources, and is often criticized for being “egalitarian version” of free market approach and unable to address other systemic forms of inequalities, such as racial or gender inequality. See NUSSBAUM, *supra* note 635 at 56–58. Much has been written about how algorithmic power exacerbates particularly racial or gender inequalities, and forms of oppression. See e.g., VIRGINIA EUBANKS, *AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH* (2019). See also CATHY O’NEIL, *WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY* (2017). Crawford captures breadth and depth of societal issues raised by algorithmic power that are not necessarily egalitarian welfare problems, See generally KATE CRAWFORD, *ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE* (2021).

⁷³¹ See DE GREGORIO, *supra* note 154 at 3.

⁷³² See for an overview of the processes, and also taken philosophical approaches Luciano Floridi, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, 34 *PHILOS. TECHNOL.* 215 (2021).

⁷³³ Capability Approach has been largely developed by Amartya Sen and Martha Nussbaum to deal with the issue of measuring the development of the countries. Traditionally Gross Domestic Product has been adopted to measure the well-being of people and their quality of life. Sen and

market economy – to maximize people’s well-being in any given society.⁷³⁴ However, this approach expands the notion of well-being from economic welfare to a broader *quality of life*. It provides a tool to measure harm to the quality of life by looking at different “functionings” or types of human functioning (e.g., being healthy, being safe, being politically involved) and evaluating the extent to which people are *capable* of exercising personal autonomy with regard to those types of functioning.⁷³⁵ Moreover, the capability approach also adopts the human rights imperative of protecting basic-level human interests – it acknowledges that there are certain types of functioning about which all human beings must be able to express a certain degree of autonomy for their life to be worthy of human dignity.⁷³⁶

Instead of prescribing a rigid set of capabilities, theorists leave the list open for democratic discussion within the community.⁷³⁷ In the EU, the CFREU provides a ledger of values and interests the community deems worthy of protection in the list of human rights.⁷³⁸ Interpreting these values and interests with the aid of the capability approach normative framework provides a tool to identify harms, measure them, and qualify whether they are acceptable in the EU. This chapter uses capabilities theory to fill in the normative gaps left by purely market-based or rights-based approaches and to create a typology of consumer manipulation harms of

Nussbaum have argued for shifting focus from economic evaluations that were only one of many different proxies, to the approach that better captured people’s quality of life. *See generally*, NUSSBAUM, *supra* note 635.

⁷³⁴ Ingrid Robeyns & Morten Fibieger Byskov, *The Capability Approach*, in THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta & Uri Nodelman eds., Summer 2023 ed. 2023), <https://plato.stanford.edu/archives/sum2023/entries/capability-approach/> (last visited Apr 8, 2023). (“The capability approach is a theoretical framework that entails two normative claims: first, the claim that the freedom to achieve well-being is of primary moral importance and, second, that well-being should be understood in terms of people’s capabilities and functionings.”)

⁷³⁵ *Id.*

⁷³⁶ The difference between functionings and capabilities is of essential importance in capability approach. Capability refers to an ability to select between options and functioning to already actualized capabilities. For example, the capability to have safe and loving romantic relationships suggests the potentiality of an option to enter such relationships. In contrast, functioning refers to a person’s choice to be in such a relationship. People can also choose to be single or to organize their private life differently. Moreover, capabilities approach regards commodities such as money and material resources as instrumental to such functionings. *See* Basu Kaushik & Luis F. Lòpez-Calva, *Functionings and Capabilities*, 2 in HANDBOOK OF SOCIAL CHOICE AND WELFARE 153 (Kenneth J. Arrow, Amartya Sen, & Kotaro Suzumura eds., 2011).

⁷³⁷ While Sen avoids prescribing any specific set of capabilities altogether, Nussbaum prescribes set of ten capabilities that are very closely related to CFREU framework, and include: (1) life; (2) bodily health; (3) bodily integrity; (4) senses, imagination, and thoughts; (5) emotions; (6) practical reason; (7) affiliation; (8) other species; (9) play; and (10) control over one’s environment, that includes political participation, and participation in free market, as a consumer or entrepreneur (hereinafter Nussbaum’s Ten Capabilities). *See* NUSSBAUM, *supra* note 635 at 33–34.

⁷³⁸ *See* DUPR, *supra* note 674 at 108–110.

OBA. This typology of harms is further elaborated in section 5.2 across seven capabilities.⁷³⁹

5.2. Typology of Consumer Manipulation Harms

This thesis identifies seven types of consumer manipulation harms of OBA that are discussed in sections 5.2.1 to 5.2.7. These types of harms include *economic harms* – adverse effects on the capability to participate in the market as a consumer or an entrepreneur (section 5.2.1);⁷⁴⁰ *environment harms* – adverse effects on the capability “to live in concern for and about animals, plants, and the world of nature”, including environmental and animal welfare harms (section 5.2.2);⁷⁴¹ *affinity harms* – adverse effects on the capability to connect and be vulnerable with others, including in the online environment, and to form a social group without oppression or discrimination (section 5.2.3);⁷⁴² *privacy harms* – adverse effects on the capability to have attachments to things and people, to have emotions, and to deliberate on them without the intrusion of others (section 5.2.4);⁷⁴³ *authenticity harms* – adverse effects on the capability to make one’s own decisions and live according to one’s genuine wishes, including holding, practicing, and expressing philosophical or religious beliefs and political views (section 5.2.5);⁷⁴⁴ *integrity harms* – adverse effects on the capability to live a life of regular length, be physically and mentally healthy, and live without physical violence, emotional abuse, or behavioral conditioning (section 5.2.6);⁷⁴⁵ and *dignity harms* – adverse effects on the capability to be vulnerable (capability to develop capabilities), including capability to exercise agency without systematic threat of

⁷³⁹ The list of capabilities developed in this thesis is an updated version of Nussbaum’s Ten Capabilities to better fit the context of consumer manipulation, and also reflect CFREU values and interests. Note that, when economic harms are addressed in this thesis, private law, including consumer protection law, and competition law interpretations takes priority. When rights-based harms are addressed human rights interpretation takes priority. Capabilities approach is merely used to bind such interpretations together as a holistic overview of harms.

⁷⁴⁰ See “Control over one’s environment” in NUSSBAUM, *supra* note 635 at 36.

⁷⁴¹ See “Other species” in *Id.*

⁷⁴² See “Affiliation” in *Id.*

⁷⁴³ This capability refers to right to privacy, as well as personal data protection CFREU, *supra* note 43, Article 7, 8.

⁷⁴⁴ The capability of authenticity together with capability of decisional privacy create life lived in autonomy. Decisional privacy is the shield that enables authentic choice, manipulation violates this. Autonomy rights are protected as “Freedoms” under the Title II of the CFREU, such as freedom of thought, freedom of expression, also liberty and security.

⁷⁴⁵ This capability combines capability (2), (3), (4) from Nussbaum’s Ten Capabilities. Note however that “senses, imagination, and thoughts are taken as mental integrity. Further, this capability unifies all “dignity rights” from Title I of CFREU such as right to integrity of a person, prohibition of torture, and slavery. CFREU, *supra* note 43, arts. 2, 3, 4, 5.

instrumentalization or exploitation (section 5.2.7).⁷⁴⁶ The structure of the typology follows the hierarchy of capabilities within the capability approach, as well as a listing of interests within CFREU (dignity-solidarity), starting from the economic harms (e.g., capability to economic participation, high-level consumer protection) to dignity harms that have the highest weight.

5.2.1. Economic Harms

Consumer manipulation undermines personal autonomy concerning a person's capability for economic participation. From a market perspective, this may cause personal detriment by incurring direct economic loss (section 5.2.1.1).⁷⁴⁷ Moreover, this, at the same time, causes a structural detriment to the market (section 5.2.1.2).⁷⁴⁸

5.2.1.1 *Economic Loss: Personal Detriment*

Manipulated consumers may incur an economic loss by engaging in transactions they would not otherwise take and that do not reflect their authentic preferences.⁷⁴⁹ Such potentially unwanted transactions can happen by manipulating consumers to buy products or services that are not in their actual preferences (transaction extraction) or by manipulating consumers to pay more than they otherwise would (price extraction).⁷⁵⁰ For example, using (one or several) manipulative practices described in section 4.3.2, event organizers can target consumers' vulnerabilities (e.g., hardship targeting, affect targeting) to manipulate consumers into a temporary state of anxiety to purchase concert tickets they do not originally intend to attend.⁷⁵¹ In practice, such instances of transaction extraction can be challenging to detect. Also, the fact that a consumer has already purchased the ticket can become a precursor for updating their preferences and deciding to attend and even enjoy the concert.⁷⁵² In other cases, consumers may detect they have been manipulated, but they may discard it—for example, €10 a consumer pays for a club ticket on an upcoming Friday night may be considered a minor loss (also

⁷⁴⁶ Nussbaum does not single out this capability, but basis her capability theory on human dignity, and the idea that human beings are born vulnerable, and they are entitled of being treated as humans. See NUSSBAUM, *supra* note 635 at 19. This capability relates to Article 1 of CFREU “human dignity”. CFREU, *supra* note 43, art. 1.

⁷⁴⁷ See Zarsky, *supra* note 38 at 172.

⁷⁴⁸ See Calo, *supra* note 38 at 1025.

⁷⁴⁹ See Zarsky, *supra* note 38 at 172.

⁷⁵⁰ *Id.* See also SUNSTEIN, *supra* note 271 at 218. See also Spencer, *supra* note 295 at 991.

⁷⁵¹ See similar argument on the sale of running shoes in Zarsky, *supra* note 38 at 172.

⁷⁵² From the market perspective, if the consumer decides to attend the concert and has fun, it *can* be argued that manipulation contributes to their emotional well-being. In other words, consumer is made to do what they did not actually want, but it turns out good for them in the end.

referred to as “small and scattered damage”⁷⁵³) that cannot account for actual harm to a consumer.⁷⁵⁴

Manipulative practices of OBA may lead to uninvited price extraction – consumers may be manipulated to pay more than they otherwise would.⁷⁵⁵ For example, airlines could target consumers that they profiled to have lower levels of digital literacy or willingness to pay higher prices with advertisements for airplane tickets with higher prices than digitally literate consumers would pay.⁷⁵⁶ In practice, consumers are unlikely to detect this: airline ticket prices fluctuate for a variety of reasons, such as seat availability and departure date, and businesses can use this to cover price discrimination (e.g., *MEP6: covert personalization*).⁷⁵⁷ In addition, applied in such a way, some scholars argue that price discrimination can reward wealthier consumers at the expense of the poor, exacerbating economic inequality.⁷⁵⁸

While the economic loss is a personal detriment, it also causes a structural detriment, leading to inefficiencies in the market and causing various other harms. Such structural detriment is addressed in section 5.2.1.2.

5.2.1.2 *Market Harms: Structural Detriment*

Consumer manipulation via OBA can be exposed, and consumers can have negative experiences when they become aware of its manipulative influences

⁷⁵³ For “small and scattered damage” or “strooischade” in Dutch see W.H. VAN BOOM, B.J. DRIJBER, J.H. LEMSTRA, V.C.A. LINDIJER, T. NOVAKOVSKI, STROOISCHADE (RAPPORT I.O.V. MIN. ECONOMISCHE ZAKEN), DEN HAAG: PRDF ADVOCATEN 2009.

⁷⁵⁴ Calo, for example, finds questionable to what happens when manipulation results in purchase of a bottle of water that does not cause physical harm. See Calo, *supra* note 38 at 1026.

⁷⁵⁵ Zarsky, *supra* note 38 at 172. See also Calo, *supra* note 38 at 1026.

⁷⁵⁶ See Zuiderveen Borgesius and Poort, *supra* note 137 at 349. See also Jeffrey Moriarty, *Why Online Personalized Pricing Is Unfair*, 23 ETHICS INF. TECHNOL. 495 (2021).

⁷⁵⁷ See for an old argument about such form of price extraction in Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet* (2003). Further, see Andrew Odlyzko, *Network Neutrality, Search Neutrality, and the Never-Ending Conflict between Efficiency and Fairness in Markets*, 8 REV. NETW. ECON., 50 (2009), <https://www.degruyter.com/document/doi/10.2202/1446-9022.1169/html?lang=en> (last visited Mar 27, 2023). (“We do not know exactly what forms of price discrimination society will accept. So we should expect experimentation, *hidden as much as sellers can manage*, but occasionally erupting in protests, and those protests leading to sellers pulling back, at least partially. And occasionally we should expect government action, when the protests grow severe.”)

⁷⁵⁸ See an argument about “regressive distribution effects” in Laura Moy & Amanda Conley, *Paying the Wealthy for Being Wealthy: The Hidden Costs of Behavioral Marketing (Unpublished Manuscript)*, <https://sites.law.berkeley.edu/privacylaw/2013/05/24/laura-moy-amanda-conley-paying-the-wealthy-for-being-wealthy-the-hidden-costs-of-behavioral-marketing/> (last visited Mar 27, 2023). See also Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users’ Information*, WALL STREET JOURNAL, Dec. 24, 2012, (last visited Mar 27, 2023).

(section 5.2.4).⁷⁵⁹ For example, a person who visits a mental health-related website and is later targeted by a related advertisement may experience stress and anxiety.⁷⁶⁰ In one example, *BetterHelp*, an online counseling service, has repeatedly and covertly disclosed consumers' mental health information to Facebook and other platforms for OBA purposes.⁷⁶¹ In general, due to the prevalence of manipulative practices, consumers worry about how their personal information is used and may feel vulnerable online.⁷⁶² Exposure to manipulative practices may significantly reduce consumers' trust in markets through negative subjective experiences of their own or general awareness of such practices online.⁷⁶³ For example, the consumer may think that other online counseling services also share their data with third parties and decide not to seek their services.

Consumers may lose trust in online markets, withdraw from valuable services, and adversely affect consumer welfare.⁷⁶⁴ The reduction of consumer trust may also be harmful from a distributive fairness perspective – poor, elderly, individuals with physical and mental disabilities, illiterate or digitally illiterate (people who lack skills to navigate the digital world) are perhaps more vulnerable to such experiences, causing them to be cut off from valuable digital services.⁷⁶⁵ For example, a person who avoids seeking in-person counseling due to the associated stigma of the community (in their country of residence) towards mental health issues may feel anxious about losing control over their mental health information and decide not to use online counseling services that could otherwise provide crucial support for their well-being (section 5.2.3).

⁷⁵⁹ See e.g., *Consumer Scoreboard*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/e/ip_23_1891 (last visited Mar 30, 2023).

⁷⁶⁰ See also Zarsky, *supra* note 38 at 173.

⁷⁶¹ FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, FEDERAL TRADE COMMISSION (2023), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook> (last visited Mar 30, 2023). (“According to the complaint, BetterHelp pushed consumers to hand over their health information by repeatedly showing them privacy misrepresentations and nudging them with unavoidable prompts to sign up for its counseling service.”)

⁷⁶² *Consumer Scoreboard*, *supra* note 759. (“With regards to online advertising in particular, 94% [of consumers] expressed concerns about it, with 70% worried about inappropriate use and sharing of personal data, 66% about the collection of online data and related profiling without explicit knowledge or agreement and 57% about cookies' installation.”)

⁷⁶³ See Zarsky, *supra* note 38 at 173. (“[Consumers] might even opt to shun the relevant market altogether due to their loss of trust in the vendor's conduct, while assuming that other vendors will follow suit.”)

⁷⁶⁴ See about the importance of consumer trust in online markets in Yassine Jadil, Nripendra P. Rana & Yogesh K. Dwivedi, *Understanding the Drivers of Online Trust and Intention to Buy on a Website: An Emerging Market Perspective*, 2 INT. J. INF. MANAG. DATA INSIGHTS 100065 (2022).

⁷⁶⁵ See Zarsky, *supra* note 38 at 173.

Consumers aware of manipulative practices in the online environment may decide to circumvent them by investing (their time and money) in avoidance measures.⁷⁶⁶ For example, consumers may install *ad-blockers* or *Virtual Private Networks (VPNs)* to help them avoid being tracked or presented by advertisements.⁷⁶⁷ Avoidance measures may reduce consumer welfare in various ways: for example, some ad-blockers are available for free and block advertisements but leave tracking possible.⁷⁶⁸ Such free ad-blockers may expose consumers to cybersecurity threats (e.g., malware).⁷⁶⁹ In contrast, paid ad-blockers, often provided with VPN services, may cost around €3 per month.⁷⁷⁰ This does not protect against manipulative advertising but all advertising, taking away valuable devices from a market perspective.⁷⁷¹ In sum, manipulative practices of OBA, even when they do not successfully manipulate consumers, can lead to a loss of consumer trust and, therefore, a decrease in consumer welfare.⁷⁷²

Moreover, looking at manipulative practices of OBA in isolation, for example, by evaluating consumer harms of an individual cookie banner dark pattern, misses one of the central issues of consumer manipulation via OBA, a phenomenon this thesis refers to as a “consumer manipulation market trap.” This phenomenon arises as the gatekeepers lock in other businesses, including providers of other platforms, publishers, and advertisers, into an advertisement configuration and infrastructure that continues to extract surplus from consumers via manipulation.⁷⁷³ Since adopting OBA as their business model, gatekeepers, such as Alphabet and Meta, have generated unprecedented revenue, part of which they have extracted through manipulative practices on their platforms.⁷⁷⁴ For example, Alphabet covertly scanned Gmail messages for selling advertisements until 2017, and Meta identified

⁷⁶⁶ See Calo, *supra* note 38 at 1027.

⁷⁶⁷ See Zarsky, *supra* note 38 at 187. See also Calo, *supra* note 38 at 1027. See generally Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy’s Price*, 90 N. C. LAW REV. (2012).

⁷⁶⁸ See generally Tolga Tekbasan, *The Effects of Ad-Blocking on the Online Customer Behavior* (University of Twente, Master Thesis, 2019), <https://essay.utwente.nl/79763/>.

⁷⁶⁹ See Lee Mathews, *A Dangerous Flaw In Popular Ad Blockers Put 100 Million Users At Risk*, FORBES (2019), <https://www.forbes.com/sites/leemathews/2019/04/17/a-dangerous-flaw-in-popular-ad-blockers-put-100-million-users-at-risk/> (last visited Mar 30, 2023).

⁷⁷⁰ See, e.g., *VPN cost?*, NORDVPN (2022), <https://nordvpn.com/pricing/> (last visited Mar 29, 2023). See, e.g., *AdBlock VPN: Get It Now*, ADBLOCK VPN, <https://vpn.getadblock.com/en/purchase/> (last visited Mar 30, 2023).

⁷⁷¹ The Cost of Ad Blocking, DARKPONY DIGITAL, <https://www.darkpony.com/blog-en/the-cost-of-ad-blocking/> (last visited Mar 30, 2023). (“Ad block usage in the United States resulted in an estimated \$5.8B in blocked revenue during 2014.”)

⁷⁷² Zarsky, *supra* note 38 at 187. See also Calo, *supra* note 38 at 1027.

⁷⁷³ Zuboff describes the emergence of the “behavioral futures markets” in which Alphabet and Meta maintain dominance by building “moat around the castle”. See for behavioral futures markets ZUBOFF, *supra* note 20 at 96–97. See for “moat around the castle” *Id.* at 98–127.

⁷⁷⁴ Trzaskowski explains that sometimes public learns about the practices platforms engage or have engaged through their announcements. See TRZASKOWSKI, *supra* note 41 at 15.

and deliberately targeted consumers' identities, such as their sexual orientation and political affiliation, on Facebook and Instagram until 2022.⁷⁷⁵

Meanwhile, providers of these platforms have consistently generated profits that surpass market predictions and set benchmarks.⁷⁷⁶ Gatekeepers have also created an infrastructure to allow other publishers to join and benefit from the surplus profits of OBA configuration.⁷⁷⁷ This infrastructure traps all other businesses into joining: not participating in an OBA infrastructure and not allowing the OBA configuration can be detrimental for publishers and advertisers whose competitors may collect excess profits.⁷⁷⁸ As the OBA configuration and the excess profits it allows require the sharing of consumer information, these businesses (including publishers and advertisers) compete for consumer manipulation and have populated the entire online environment with manipulative practices.⁷⁷⁹ Nevertheless, having access to most of consumers' attention, time, and data online, gatekeepers maintain the position of power in this consumer manipulation market

⁷⁷⁵ See for Google's Gmail scanning Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*, WSJ (2018), <https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442> (last visited Mar 30, 2023). See also As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align, GOOGLE (2017), <https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/> (last visited Mar 30, 2023). See for Facebook's identity targeting Mike Isaac & Tiffany Hsu, *Meta Plans to Remove Thousands of Sensitive Ad-Targeting Categories.*, THE NEW YORK TIMES, Nov. 9, 2021, <https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html> (last visited Mar 30, 2023). (“[...] Meta has often struggled with how to take advantage of consumer data without abusing it.”) See also *Removing Certain Ad Targeting Options and Expanding Our Ad Controls*, META FOR BUSINESS, <https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls> (last visited Mar 30, 2023).

⁷⁷⁶ UK's CMA analyzed profitability of these platforms through return-on-capital employed (ROCE) to measure profitability of these companies. CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 67. (“We have found through our profitability analysis that the global return on capital employed for both Google and Facebook has been well above any reasonable benchmarks for many years.”)

⁷⁷⁷ See ZUBOFF, *supra* note 20 at 82–85.

⁷⁷⁸ See European Commission Study Recent Digital Advertising Developments, *supra* note 433 at 136. See Stigler Committee, *Digital Platforms: Final Report* 336, 62 (2019).

⁷⁷⁹ During this writing, majority of websites online employ manipulative practices, at least in (but not limited to) the context of cookie banners. See *More Cookie Banners to go: Second wave of complaints underway*, NOYB, <https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway> (last visited Mar 30, 2023). See also Midas Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence*, in PROCEEDINGS OF THE 2020 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1, 10 (2020), <http://arxiv.org/abs/2001.02479> (last visited Mar 29, 2023). See also European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53 at 6. (“According to the mystery shopping exercise, 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern.”) Note that consumer manipulation market refers to the incentive of publishers and advertisers to adopt manipulative practices in order to gain OBA's excess profit, and “trap” refers to their dependance on continuing this practice.

and are its primary beneficiaries, as both publishers and advertisers depend on them for their profits.⁷⁸⁰

Such a consumer manipulation market trap *inhibits innovation*, making it improbable that new forms of digital services can emerge that can revolutionize society as online platforms of the gatekeepers such as Alphabet and Meta once did.⁷⁸¹ In particular, such a market trap makes it difficult for autonomy-preserving alternatives to emerge: it is unlikely that such alternatives can compete with businesses that generate revenue through consumer manipulation that extracts excess profits.⁷⁸² Such a trap and reduced innovation can also decrease the overall *quality* of digital services and content consumers receive.⁷⁸³ In the *laissez-faire* market, which is free and competitive, businesses have an incentive to continuously increase the quality of their service to satisfy the demands of ever-evolving consumer preferences.⁷⁸⁴ Businesses that face the risk of competitors increase the quality of their services by offering new functionalities users may find more valuable (e.g., easier to use) or lower prices to increase consumer welfare.⁷⁸⁵ However, consumer manipulation via OBA allows businesses to continue to extract surplus from consumers without improving quality, arguably resulting in lower-quality digital services.⁷⁸⁶ One study measures such a reduction in quality by

⁷⁸⁰ European Commission Study Recent Digital Advertising Developments, *supra* note 433 at 136. (“Advertisers are highly reliant on data to measure the performance of ads, but say they have difficulty accessing it, especially when working with Google and Meta. This had led to a lack of trust. Several advertisers also feel that they do not have enough information about how Google sets its prices. [...] Publishers described Google and Meta as their most important competitors, as they are often perceived by advertisers as simpler and sometimes cheaper options for digital advertising. Publishers explained that they struggle to compete with large platforms for reasons primarily related to data, reach and pricing. Platforms are seen as an easy way for advertisers to reach large numbers of potential customers.”)

⁷⁸¹ CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 308. (“Google and Facebook themselves were able to emerge, with limited resources, on the back of a good idea, producing new and innovative services that [...] are highly valued by consumers. We are concerned that, without reform, existing market dynamics will mean that the next great innovation cannot emerge to revolutionize our lives in the way that Google and Facebook have done in the past.”) Note however, that the emergence of ChatGPT was the first time threatening Google Search dominance. As of Meta’s Facebook and Instagram, TikTok has risen as its major competitor that also employs OBA as its central business model.

⁷⁸² *Id.* at 311. See similar argument in Stigler Committee, *supra* note 778 at 62.

⁷⁸³ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 313.

⁷⁸⁴ *Id.*

⁷⁸⁵ *Id.*

⁷⁸⁶ *Id.* See also European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 39.

looking at the number of advertisements shown to the consumers – Instagram, for example, increased ad impressions by 200% in 2019 compared to 2016.⁷⁸⁷

Consumer manipulation via OBA can also be evaluated from the *total welfare* standard. Such a market-based perspective requires the inclusion of all consumer harms into cost-benefit analyses that consider the profit the businesses have derived from consumer manipulation via OBA.⁷⁸⁸ Such a view may suggest that consumer manipulation via OBA is justifiable because while consumer manipulation via OBA causes consumers to be distracted, lose time, and occasionally buy things they do not need, it also creates a business model that enables free services such as WhatsApp, Gmail, and Google Maps, which have become essential for many consumers. In other words, the total welfare perspective may justify tolerating autonomy-undermining technology because it increases overall welfare in the long run.⁷⁸⁹

Authoritative studies from the EU, UK, and US that attempted to measure the total economic effects of the OBA infrastructure suggest that it may reduce the overall welfare of consumers when it leads to anti-competitive effects that this thesis conceptualizes as the consumer manipulation market trap.⁷⁹⁰ These studies argue that while OBA allows consumers to access digital services and content without monetary payment, OBA favors large platforms with data advantages, causing a lack of competition and decreased returns to consumers. It is even argued that without the anticompetitive effects of OBA, consumers could profit monetarily (or through other rewards) for accessing digital services and content.⁷⁹¹

The indicator of this potential is revealed in the amount of excess profit generated by the gatekeepers that exceed all market predictions and set benchmarks—the UK’s CMA found that only in 2018, Alphabet and Meta earned £2 billion more profit than what was required for fair returns to shareholders.⁷⁹² The reports of competition authorities suggest that, without the anti-competitive effects of their

⁷⁸⁷ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 313.

⁷⁸⁸ See Stigler Committee, *supra* note 778 at 66.

⁷⁸⁹ *Id.* at 64. (“We caution, however, that the legal structure of US antitrust law is not well set up to accommodate this complexity as it opens the door for judges to weigh all manner of social concerns as well as traditional economic effects.”)

⁷⁹⁰ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 70. See generally Stigler Committee, *supra* note 778. See also DIGITAL COMPETITION EXPERT PANEL, *Unlocking Digital Competition: Report of the Digital Competition Expert Panel* (2019). See CNMC (Spain) Study Competition in Online Advertising, *supra* note 34 at 148–189.

⁷⁹¹ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 70, 317.

⁷⁹² *Id.*

business model (which this thesis identifies as manipulative practices of OBA), such excess profits would have been shared amongst consumers.⁷⁹³

Lastly, the consumer manipulation market trap can contribute to increased prices for goods and services that are being advertised.⁷⁹⁴ Gatekeepers that generate surplus profits from the consumer manipulation market heavily tax advertisers and publishers in the OBA industry for relying on their advertising intermediation.⁷⁹⁵ As a result, higher advertising prices increase prices for goods and services for consumers.⁷⁹⁶

5.2.2. Environment Harms

Consumer manipulation via OBA can exacerbate environmental harms by adversely affecting the Earth's ecology or the welfare of the animals sharing the planet with human beings.

As OBA requires large data centers and servers to store and process swaths of consumer behavioral data, it consumes vast energy and has a significant CO₂ footprint.⁷⁹⁷ One study calculates the yearly carbon impact of the online advertising industry to be around 60 million tonnes (Mt) of CO₂, seven times more than the emissions of the Netherlands in 2021.⁷⁹⁸ Also, these data centers require much water, which sometimes takes away supply from communities with limited access to water.⁷⁹⁹ While no data is available to measure how much *consumer manipulation* contributes to such environmental impact, its exacerbating effect is undeniable – manipulative extraction practices such as infinite scrolling extract more data and

⁷⁹³ See *Id.* ⁷⁹³ See Stigler Committee, *supra* note 778 at 91. See generally Veronica Marotta et al., *The Welfare Impact of Targeted Advertising Technologies*, 33 INF. SYST. RES. 131 (2022).

⁷⁹⁴ See Stigler Committee, *supra* note 778 at 91. See European Parliament Study Online Advertising & Consumer Choice, *supra* note 36 at 39. See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 313.

⁷⁹⁵ See European Commission Study Personalization, *supra* note 33 at 24. (“Intermediary services can typically charge a fee of up to 12% of the cost of an ad impression.”)

⁷⁹⁶ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33 at 314.

⁷⁹⁷ See generally Patrick Hartmann et al., *Perspectives: Advertising and Climate Change – Part of the Problem or Part of the Solution?*, 42 INT. J. ADVERT. 430 (2023). See generally Matti Pärssinen et al., *Environmental Impact Assessment of Online Advertising*, 73 ENVIRON. IMPACT ASSESS. REV. 177 (2018).

⁷⁹⁸ Between 12Mt and 159Mt EqCO₂ when considering uncertainty. See Pärssinen et al., *supra* note 797 at 177. See Hannah Ritchie, Max Roser & Pablo Rosado, *Netherlands: CO₂ Country Profile*, OUR WORLD DATA (2020), <https://ourworldindata.org/co2/country/netherlands> (last visited Apr 10, 2023). See also Kimberley Derudder, *What Is The Environmental Footprint For Social Media Applications? 2021 Edition*, GREENSPECTOR (2021), <https://greenspector.com/en/social-media-2021/> (last visited Apr 10, 2023).

⁷⁹⁹ See Nikitha Sattiraju, *Secret Cost of Google's Data Centers: Billions of Gallons of Water* (2020), <https://time.com/5814276/google-data-centers-water/> (last visited Jul 5, 2023).

attention, while manipulative personalization leads to needless transactions.⁸⁰⁰ Exaggerated consumption that leads to the extraction of attention and time causes faster drainage of the batteries on consumer devices, contributing to significant electronic waste.⁸⁰¹ At the same time, needless economic purchase decisions contribute to needless consumerism, which has the most significant impact on global greenhouse emissions.⁸⁰²

Consumer manipulation via OBA can also affect consumers' relationships with other species.⁸⁰³ It may have positive effects on animal welfare—for example, social media has contributed to the increase in pet adoption rates.⁸⁰⁴ However, consumer manipulation via OBA can also harm animal welfare in at least four ways. Consumers increasingly acquire pets through online ads that allow them immediate access to young and fashionable pets, unlike physically verified sources with a limited supply of pets that take more time.⁸⁰⁵ While the online pet trade is booming, most dogs, cats, and exotic wild animals arrive online through illegal cross-border trade.⁸⁰⁶ Such illegal trade can affect animal welfare and health through an increased risk of dehydration, heat stress, the spread of infectious diseases, and cosmetic surgeries that result in highly fearful animals.⁸⁰⁷ OBA gives illegal trades increased capability to exploit consumers' desires for pet adoption, leading to harm to animal welfare.

⁸⁰⁰ See Lindsay Dodgson, *Why TikTok Makes the Hours Seem to Melt Away, According to Experts Who Study How Our Brains Perceive Time*, INSIDER, Jul. 26, 2022, <https://www.insider.com/why-time-passes-so-quickly-scrolling-on-tiktok-2022-7> (last visited Apr 10, 2023).

⁸⁰¹ Pärssinen et al., *supra* note 797 at 181.

⁸⁰² More than 70% of global greenhouse emissions directly arise from consumption decisions. Hartmann et al., *supra* note 797 at 430.

⁸⁰³ Generally, social media has impacted the way humans perceive animals. *See generally* Elizabeth Riddle & Jill R. D. MacKay, *Social Media Contexts Moderate Perceptions of Animals*, 10 ANIM. OPEN ACCESS J. MDPI 845 (2020).

⁸⁰⁴ See Jacey Birch, *Social Media Now Having Influence on Pet Adoptions*, WPLG (2023), <https://www.local10.com/news/local/2023/02/28/social-media-now-having-influence-on-pet-adoptions/> (last visited Apr 10, 2023).

⁸⁰⁵ EUROGROUP FOR ANIMALS, *The Illegal Pet Trade: Game Over*, 22 (June 2020).

⁸⁰⁶ *Id.*

⁸⁰⁷ Digital Services Act: How Does It Protect Animals From The Illegal Online Trade?, EUROGROUP FOR ANIMALS, <https://www.eurogroupforanimals.org/news/digital-services-act-how-does-it-protect-animals-illegal-online-trade> (last visited Apr 10, 2023). (“During transport, many welfare issues arise such as risk of dehydration and heat stress, lack of enough space to be able to stand/lay down, high potential for spreading of infectious diseases among the transported animals and beyond, and a higher likelihood of pregnant dogs & cats transported too close to their estimated due dates to name but a few. In relation to breeding practices, cosmetic and convenience surgeries vastly performed outside the EU, resulting in severe pain and impairing of social communication (through tail docking, ear cropping, debarking, declawing,...), lack of socialisation resulting in extreme fearful and anxious animals, lack of genetic variation as a consequence of inbreeding leading to poor health and unfitness to carry a normal life.”)

In sum, the impact on the environment and animal welfare of a single manipulative practice may be minuscule, but the aggregate effect of these manipulative practices has significant potential to affect the globe, decrease animal welfare, and adversely affect how humans relate to other species and the world around them.

5.2.3. Affinity Harms

OBA can lead to discriminatory advertising delivery, such as excluding particular groups from advertisements that offer essential opportunities, such as employment or housing.⁸⁰⁸ For example, in job advertisements, OBA campaigns have favored men over women.⁸⁰⁹ In another example, inferring racial identity from people's names has had a discriminatory effect on people's employment opportunities.⁸¹⁰ Studies have demonstrated that the discriminatory outcomes of OBA directly stem from the spillover of socially existing biases in the relevance optimization algorithm, linking the discrimination harms to OBA's manipulative imperative.⁸¹¹ OBA has also allowed advertisers to include and exclude traditionally marginalized groups in advertising campaigns, leading to further discrimination and oppression. For example, Facebook has been used to target young LGBTQ+ users with "gay cure" advertisements.⁸¹² Such targeting is, in essence, manipulative as it exploits consumers' vulnerabilities and is oppressive and discriminatory, affecting the person's sense of belonging to a group and society.

Providers of the largest platforms, such as Alphabet and Meta, have removed the possibility in their OBA configuration to target groups explicitly profiled into categories relating to race, ethnicity, and sexual orientation.⁸¹³ However, this does not mean that the optimization algorithm does not implicitly infer such categories.⁸¹⁴ In particular, the feat of "lookalike" or "similar" audiences can group people according to the similarity of their online behavior without explicitly naming them as related to sensitive categories – having exploitative and discriminatory effects that can also be disguised under algorithmic neutrality.⁸¹⁵ Lastly, consumer

⁸⁰⁸ See generally Wachter, *supra* note 80.

⁸⁰⁹ L. Elisa Celis, Anay Mehrotra & Nisheeth K. Vishnoi, *Toward Controlling Discrimination in Online Ad Auctions* (2019), <http://arxiv.org/abs/1901.10450> (last visited Apr 10, 2023).

⁸¹⁰ See Latanya Sweeney, *Discrimination in Online Ad Delivery - ACM Queue*, 11 ACM DIGIT. LIBR. 10 (2013).

⁸¹¹ Muhammad Ali et al., *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3 PROC. ACM HUM.-COMPUT. INTERACT. 1 (2019).

⁸¹² See Zard and Sears, *supra* note 1 at 839. See also Wachter, *supra* note 80 at 378.

⁸¹³ See e.g. Removing Certain Ad Targeting Options and Expanding Our Ad Controls, *supra* note 775. See Personalized Advertising, *supra* note 120.

⁸¹⁴ See Zard and Sears, *supra* note 1 at 835.

⁸¹⁵ See Wachter, *supra* note 80 at 401.

manipulation may lead to exacerbating economic inequalities by exploiting low-income people.⁸¹⁶

Such discrimination and oppression impair the right to non-discrimination protected by the Article 21 of the Charter of Fundamental Rights of the EU (CFREU).⁸¹⁷

5.2.4. Privacy Harms

Manipulative practices of OBA do not always lead to successful manipulation, but consumers sometimes identify them as manipulative. Whether they are successful or not, they violate consumers' *privacy*. For example, the consumer who sees an advertisement for online counseling may guess that they have been targeted because a mental health-related website covertly shared the information with an advertising platform. In such cases, an advertisement violates consumers' *informational privacy* because it accesses consumers' personal information against their wishes.⁸¹⁸ Manipulative advertising practices also undermine consumers' *decisional privacy* – as they attempt to influence consumer choices hiddenly.⁸¹⁹ Decisional privacy provides essential breathing space to make authentic choices and exercise personal autonomy.⁸²⁰ In response to becoming aware of interferences with their decisional privacy, consumers may experience *emotional distress*, such as “annoyance, frustration, fear, embarrassment, anger, and various degrees of anxiety”.⁸²¹ Many of the manipulative practices of OBA also act as *disturbances* to consumers' piece of mind, similar to telemarketing communications.⁸²² As a result, consumers often experience OBA as “creepy” and “intrusive”.⁸²³

⁸¹⁶ See an argument about “regressive distribution effects” in Moy and Conley, *supra* note 758. See also Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL STREET JOURNAL, Dec. 24, 2012, (last visited Mar 27, 2023). Ariel Ezrachi & Maurice E. Stucke, *The Rise of Behavioural Discrimination*, 37 EUR. COMPET. L. REV. 484 (2016).

⁸¹⁷ Consolidated Version of the Charter of Fundamental Rights of The European Union, October 26, 2012, O.J. (C326)391 [hereafter CFREU], *supra* note 520 at 21.

⁸¹⁸ See generally WESTIN, *supra* note 694. See also Marolijn Lanzing, *The Transparent Self: A Normative Investigation of Changing Selves And Relationships In The Age Of Quantified Self* (University of Eindhoven, Dissertation, 2019).

⁸¹⁹ See ROESSLER, *supra* note 636 at 9. See also Marolijn Lanzing, *supra* note 820 at 75. (“Decisional privacy is broadly defined as the right to defend against unwanted access and interference in our decisions and actions. Roughly, ‘being interfered with’ means that (un)known actors or entities have access to one’s behaviour and decisions, which allows them to comment upon, interpret or change one’s behaviour and steer one’s decisions, while this access does not fall under the reasonable expectations of the user or subject or was not granted in the first place.”)

⁸²⁰ See Marolijn Lanzing, *supra* note 820 at 75–76.

⁸²¹ See Citron and Solove, *supra* note 625 at 841.

⁸²² *Id.* at 846.

⁸²³ See de Groot, *supra* note 555 at 62.

Using the information consumers did not intend to provide or expect to be used for targeting thwarts their expectations of privacy.⁸²⁴ The “reasonable expectation of privacy” is a benchmark in the EU human rights framework for analyzing treatment regarding people’s privacy that they are entitled to.⁸²⁵ Collecting information about consumers without their knowledge violates such entitlements. As a result of thwarted expectations, consumers may lose the sense that they are in control of information about themselves.⁸²⁶ Indeed, such information can be used against consumers’ interest in many ways: for example, mental health information can be accessed by others, causing consumer reputational damage or affecting their relationships. Therefore, such loss of control disables consumers from managing risks related to their information and can lead to anxiety.⁸²⁷

The EU human rights framework protects individuals’ informational and decisional privacy under the rights of private life and personal data protection. Privacy harms, however, can also be relevant from a market-based perspective. Consumers can theoretically request compensation for psychological detriment or the emotional cost of these practices.⁸²⁸ This can be particularly difficult to quantify due to the nature of consumer manipulation harms that are often “small and scattered.” Each instance potentially causes small distress, and these instances can be completely unrelated as they emerge from different actors.

5.2.5. Authenticity Harms

Consumer manipulation via OBA can lead to potentially unwanted transactions with direct economic loss, but this is not always the case. However, it always leads to loss of *time*, and thus, manipulation can be understood as time theft.⁸²⁹ By interacting with manipulative practices, consumers spend more time online than without such influence.⁸³⁰ Human time is of essential importance under the EU human rights framework.⁸³¹ The principle of *self-determination* that stems from the human dignity root of this framework can be interpreted as the “freedom to construct one’s own time.”⁸³² It protects authenticity conditions of personal autonomy, including decisions about how to spend one’s time in accordance with

⁸²⁴ See Citron and Solove, *supra* note 625 at 851.

⁸²⁵ Perry v. United Kingdom, no 63737/00, ECHR 2003-IX. See also Benedik v. Slovenia, no. 62357/14 (ECHR, 24 April 2018).

⁸²⁶ See Citron and Solove, *supra* note 625 at 851.

⁸²⁷ *Id.* at 854.

⁸²⁸ See European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 649 at 40.

⁸²⁹ Cass R. Sunstein, *Manipulation As Theft* (2021), <https://papers.ssrn.com/abstract=3880048> (last visited Mar 20, 2023).

⁸³⁰ The Commission Dark Patterns and Manipulative Personalisation Study, *supra* note 36 at 90.

⁸³¹ See DUPR, *supra* note 674 at 141–170.

⁸³² *Id.* at 152.

the “self”.⁸³³ The German constitutional tradition refers to this as “the right to free development of personality,” which also protects the interest of personal data protection right emerging in the EU.⁸³⁴ Consumer manipulation undermines such authenticity interest by taking away the capability to construct one’s own time.⁸³⁵

While the CFREU nor the ECHR do not explicitly list such a right to authenticity, this principle permeates many of the “freedom rights” in Title II. The “freedom of thought, belief and religion” is a particularly relevant right that consumer manipulation can directly impair by limiting consumers’ capability to hold religious beliefs authentic to them. For example, the *Mormon Ads* campaign mentioned in section 4.3.2 demonstrated that OBA could manipulate consumers to change their life-long religious beliefs.⁸³⁶ Consumer manipulation can also have *chilling effects* on “freedom of expression” – consumers often use digital services, such as social media, to express their authentic selves, including political opinions. Nevertheless, either through interruptions or through causing emotional distress, manipulative practices may trigger consumers to avoid voicing their options or being on social media altogether.

One can also speculate that consumer manipulation challenges the “right to liberty and security”. However, such an argument that consumer manipulation via OBA crosses the legal threshold of this right that protects individuals from arbitrary detentions by the state would be difficult to defend for three reasons.⁸³⁷ Firstly, in contrast to the state’s coercive deprivation of liberty by arbitrary arrest, the magnitude of spending time online against one’s authentic wishes is, intuitively, relatively smaller. Secondly, even when taking time as a measure, instances of consumer manipulation limit the consumer’s capability for authentic action by minuscule amounts of time. It is also challenging to aggregate these instances into overall time-theft that happens through often competing actors in various unrelated contexts.

⁸³³ ROESSLER, *supra* note 636. See also Dupr, 155 (“[Human dignity] can be further understood as promoting the acknowledgement and protection of individual identities and human personalities.”)

⁸³⁴ See Grundgesetzes[GG][Basic Law], translation at: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html (accessed October 31, 2023)., 2. See also BVerfG, 1 BvR 209/83, Dec. 15, 1983, *supra* note 655.

⁸³⁵ Franklin et al., *supra* note 39. Casey Newton, ‘Time Well Spent’ Is Shaping up to Be Tech’s next Big Debate, THE VERGE (2018), <https://www.theverge.com/2018/1/17/16903844/time-well-spent-facebook-tristan-harris-mark-zuckerberg> (last visited Mar 29, 2023).

⁸³⁶ Faddoul, Kapuria, and Lin, *supra* note 457 at 4.

⁸³⁷ See James Griffin, *Autonomy*, in ON HUMAN RIGHTS (James Griffin ed., 2008), <https://doi.org/10.1093/acprof:oso/9780199238781.003.0009>. EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 5 of the European Convention on Human Rights* (2022).

In 2022, social media users spent more than two hours daily on average on social networking sites.⁸³⁸ Manipulative practices in the online environment are sometimes attributed the role of distractors that largely contribute to such time spent on social networking services.⁸³⁹ However, there is no empirical data available that quantifies the extent to which manipulative practices contribute to the increasing amounts of time people spend online.

From a market perspective, loss of time can be detrimental to the consumer via the loss of opportunities, for example, *loss of earnings* due to losing time consumers could spend at work.⁸⁴⁰ The market approach also recognizes the *loss of consortium* as the time lost that could have been spent in interpersonal relationships, as well as *leisure*, more broadly.⁸⁴¹ Similar to ad-blockers, new tools have emerged for consumers to protect their time, making time loss a tangible harm of consumer manipulation.⁸⁴²

5.2.6. Integrity Harms

In order for people to construct time of their own and live autonomous, authentic lives, they need to have a certain level of health and specific physical and mental capabilities.⁸⁴³ Market-based and rights-based approaches protect such capabilities. Consumer manipulation can undermine consumers' physical and mental integrity in a variety of ways. Consumer manipulation can lead to purchasing goods that can harm one's health ("demerit goods").⁸⁴⁴ For example, consumer manipulation can lead to physical injury by promoting excessive consumption of products and services, such as cigarettes, alcohol, junk food, gambling, or pornography.⁸⁴⁵ Such detriment is also recognized from the market-based perspective that sees an increased sale of demerit goods as an externality that leads to market failure.⁸⁴⁶

⁸³⁸ See *Global daily social media usage 2022*, STATISTA, <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/> (last visited Mar 29, 2023).

⁸³⁹ See OLIVER BURKEMAN, *FOUR THOUSAND WEEKS: TIME MANAGEMENT FOR MORTALS* (2021).

⁸⁴⁰ See European Commission Study *Dark Patterns & Manipulative Personalization*, *supra* note 649 at 25.

⁸⁴¹ *Id.* at 39.

⁸⁴² *RescueTime: Fully Automated Time Tracking Software*, RESCUETIME, <https://www.rescuetime.com/> (last visited Apr 1, 2023).

⁸⁴³ Griffin, *supra* note 839.

⁸⁴⁴ Demerit goods are contrasted with "merit goods" that authorities want to see greater consumption of. See Richard A. Musgrave, *Merit Goods*, in *THE NEW PALGRAVE DICTIONARY OF ECONOMICS 1* (2017), https://doi.org/10.1057/978-1-349-95121-5_1139-2 (last visited Mar 28, 2023).

⁸⁴⁵ See Calo, *supra* note 38 at 1025.

⁸⁴⁶ *Id.*

The online environment permeated with manipulative practices leads to increased impulsivity and compulsive behavior.⁸⁴⁷ In some cases increase in impulsivity has been argued to lead to certain behavioral addictions, such as “porn addiction” or “social media addiction”, imposing systematic limitations on consumer behavior and authentic choice.⁸⁴⁸ To maximize the consumer’s time spent online, some practices, such as content personalization, may adversely affect the consumer’s self-esteem.⁸⁴⁹ The issues of self-image can be developed into full-fetched body self-image issues.⁸⁵⁰ One such effect, for example, has been labeled as “Snapchat Dysmorphia”.⁸⁵¹ Such body-dysmorphic effects significantly increase cosmetic surgeries to which OBA’s manipulative practices have undeniably contributed.⁸⁵²

Systematic exposure to manipulative practices (e.g., covert personalization, infinite scroll, auto-play) can also cause and exacerbate mental health issues. It is closely linked to an increase in anxiety and depression symptoms. In extreme cases, this may lead to self-harm and even death. In one real-life case from the United Kingdom, the coroner who examined the death of fourteen-year-old Molly Powel suggested that the personalization algorithm that exacerbated her depression was the direct cause of her self-harm and eventual suicide.⁸⁵³ This case illustrates the potential of consumer manipulation to threaten the essential core of human rights interests, such as human life and physical and mental integrity. The CFREU draws a clear boundary for the minimum core quality of life at the physical and mental health and integrity.⁸⁵⁴ Crossing this line constitutes the mistreatment of consumers in a way that is not worthy of their dignity as human beings.⁸⁵⁵

5.2.7. Dignity Harms

Consumer manipulation in the online environment can also be seen as an affront to the *dignity* of individuals, which envelops the most significant harms of consumer manipulation.⁸⁵⁶ The dignity argument typically refers to the

⁸⁴⁷ Maartje Boer et al., *Attention Deficit Hyperactivity Disorder-Symptoms, Social Media Use Intensity, and Social Media Use Problems in Adolescents: Investigating Directionality*, 91 CHILD DEV. 853 (2020).

⁸⁴⁸ See Qinghua He, Ofir Turel & Antoine Bechara, *Brain Anatomy Alterations Associated with Social Networking Site (SNS) Addiction*, 7 SCI. REP. 45064 (2017).

⁸⁴⁹ See Susruthi Rajanala, Mayra B. C. Maymone & Neelam A. Vashi, *Selfies—Living in the Era of Filtered Photographs*, 20 JAMA FACIAL PLAST. SURG. 443 (2018).

⁸⁵⁰ See Ledger of Harms, *supra* note 48.

⁸⁵¹ See Rajanala, Maymone, and Vashi, *supra* note 851.

⁸⁵² See *Id.*

⁸⁵³ See Franklin et al., *supra* note 39. Molly Russell inquest, *supra* note 39; In her own words - Molly Russell’s secret Twitter account, *supra* note 39.

⁸⁵⁴ See DUPR, *supra* note 674 at 75–76.

⁸⁵⁵ *Id.*

⁸⁵⁶ See Zarsky, *supra* note 38 at 175.

instrumentalization of consumers and the undermining of the deontological “humanity formula” not to treat humans merely as a means to an end.⁸⁵⁷ Such understanding of human dignity is the core interest protected by the EU human rights framework and acts as a boundary to what is acceptable in society.⁸⁵⁸ In this framework, human dignity violations are ascribed to phenomena with adverse effects of the most significant magnitude (e.g., torture, slavery).⁸⁵⁹ Therefore, arguing that consumer manipulation via OBA undermines human dignity requires solid normative and empirical foundations.⁸⁶⁰

While observers of EU constitutionalism see developments towards the expansion of dignity to cover all economic roles of human beings, protection of “consumer dignity” is not yet definitive in the EU human rights adjudication.⁸⁶¹ Still, in the landmark *Omega Judgment*, the CJEU justified in a commercial context the prohibition of laser-tag games that simulated killing other humans because they threatened human dignity.⁸⁶² Following the court’s logic, determining dignity boundaries, including for OBA, requires evaluating whether this phenomenon poses “a genuine and sufficiently serious threat to a fundamental interest of society.”⁸⁶³ Human dignity is not only the foundational core of human rights, but the CFREU also singles out human dignity in Article 1 as a separate right, which can lead to the conclusion that dignity can be challenged directly by undermining core societal interests without necessarily violating other rights of any specific individual.

With this in mind, this section elaborates on the dignity harms of consumer manipulation via OBA in three parts: first, it addresses the threat to the dignity of a child (section 5.2.7.1); second, it addresses the threat to democracy as a core societal interest (section 5.2.7.2); and third, it addresses the systematic threat of consumer exploitation online as an affront to consumer dignity (section 5.2.7.3).

⁸⁵⁷ See KANT, *supra* note 622 at 42. (“Act in such a way that you treat humanity whether in your own person or anyone else’s, never merely as a means, but also always as an end.”) SUNSTEIN, *supra* note 271 at 84. Sunstein for example uses dignity argument to refer to consumer manipulation as a form of human experimentation, where consumers are exposed to influences they are unaware of, for goals they cannot perceive, by actors, they do not recognize.

⁸⁵⁸ See DUPR, *supra* note 674 at 75–77.

⁸⁵⁹ See *Id.* at 75.

⁸⁶⁰ Empirical argument is outside the scope of this thesis. Empirical evidence to the risks and potential of manipulation, has been very difficult to gather. However, Digital Markets Act in particular includes provisions that will give more insights into OBA practices, and possibility to evaluate harms in more empirically sound terms. Nevertheless, normatively speaking, this thesis regards existing evidence enough to conclude that consumer manipulation via at least challenges the fundamental interest in human dignity.

⁸⁶¹ Dupr discusses expansion of dignity to envisage protection of “worker’s dignity” in response to the industrial threats. For example equation of forced labour to slavery or violation of dignity is the clear expression of this. See DUPR, *supra* note 674 at 113–139. In Information Age not a worker, but a consumer is under systemic threat of exploitation, raising questions about “consumer dignity”.

⁸⁶² Case C-36/02, *Omega*, 14 October 2004, ECLI:EU:C:2004:614.

⁸⁶³ *Id.* See also Case C-54/99, *Église de Scientologie*, 14 March 2000, ECLI:EU:C:2000:124.

5.2.7.1 *Threat to Children*

Practices that extract attention, time, and data through manipulation can seriously harm *children*.⁸⁶⁴ One study found that pre-schoolers who use social media for more than one hour each day demonstrate significantly less development in brain regions involved in language and literacy.⁸⁶⁵ More screen time correlates with a lower development of social and problem-solving skills and levels of alcohol use later in life.⁸⁶⁶ Manipulative OBA practices can also lead to an increase in unhealthy food consumption by children, as well as attention problems⁸⁶⁷ and depression.⁸⁶⁸ One study shows that many children cannot adequately distinguish between facts (e.g., real news) and advertisement content.⁸⁶⁹ Therefore, their exposure to increased amounts of advertising can be detrimental to their future life decisions.⁸⁷⁰ Another study found that 85% of the YouTube videos aimed at kids below the age of eight contained advertisements, 20% of which contained violent, sexual, political, or substance-related content.⁸⁷¹

Generally, children cannot fully grasp how advertisement is targeted via OBA.⁸⁷² Manipulative personalization practices in OBA can exploit children's vulnerabilities for needless purchase behaviors. For example, in 2019, Facebook categorized 740,000 minors as interested in gambling.⁸⁷³ Such information about children can be used to exploit their impulsivity and target them with advertising

⁸⁶⁴ There has been a call for banning OBA towards children for some time now See Mie Oehlenschläger, *Open Letter: Children Are Subjected To Behavioural Advertising - End It!* · Dataetisk Tænkehandle tank, DATAETISK TÆNKEHANDLETANK (Oct. 19, 2020). See for an overview on online harms for children Ledger of Harms, *supra* note 48.

⁸⁶⁵ See John S. Hutton et al., *Associations Between Screen-Based Media Use and Brain White Matter Integrity in Preschool-Aged Children*, 174 JAMA PEDIATR. e193869 (2020).

⁸⁶⁶ See Elroy Boers, Mohammad H. Afzali & Patricia Conrod, *A Longitudinal Study on the Relationship between Screen Time and Adolescent Alcohol Use: The Mediating Role of Social Norms*, 132 PREV. MED. 105992 (2020).

⁸⁶⁷ See Susanne E Baumgartner et al., *The Relationship Between Media Multitasking and Attention Problems in Adolescents: Results of Two Longitudinal Studies*, 44 HUM. COMMUN. RES. 3 (2018).

⁸⁶⁸ See Amaal Alruwaily et al., *Child Social Media Influencers and Unhealthy Food Product Placement*, 146 PEDIATRICS e20194057 (2020).

⁸⁶⁹ Sue Shellenbarger, *Most Students Don't Know When News Is Fake, Stanford Study Finds*, WSJ, Nov. 28, 2016, <https://www.wsj.com/articles/most-students-dont-know-when-news-is-fake-stanford-study-finds-1479752576> (last visited Apr 10, 2023).

⁸⁷⁰ *Id.*

⁸⁷¹ JENNY S. RADESKY ET AL., *Young Kids and YouTube: How Ads, Toys, and Games Dominate Viewing*, 3 (2020).

⁸⁷² See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36.

⁸⁷³ Alex Hern & Frederik Hugo Ledegaard, *Children "interested in" Gambling and Alcohol, According to Facebook*, THE GUARDIAN, Oct. 9, 2019, <https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook> (last visited Apr 10, 2023).

gambling-like video games. Such online interfaces configured to facilitate OBA infrastructure raise issues regarding children’s entitlements to recreation, health, and protection from economic exploitation.⁸⁷⁴

OBA infrastructure can harm children and may constitute an affront to dignity because of systematic violation of the rights of the child enshrined in the Convention on the Rights of the Child, including a right to protection from economic exploitation (Article 32 UN CRC) and the right to play and leisure (Article 31 UN CRC).⁸⁷⁵ Further, CFREU entails taking responsibility for “future generations” as a core societal interest that comes under systematic threats in the online environment configured for OBA.⁸⁷⁶ The newer generations may find manipulative practices normal and accept practices that threaten and risk their integrity. The concept of human dignity in the EU human rights framework acts as a north star for governing change in time and as a reaffirming hope for a better future.⁸⁷⁷ Accepting that the future holds the deterioration of human capabilities can be seen as a direct threat to human dignity.

5.2.7.2 *Threat to Democracy*

Consumer manipulation via OBA has the potential to erode democratic political ordering. It can lower the *quality of journalism* by incentivizing attention-grabbing, fast-paced reporting that gets prioritized over well-researched and evidenced content that typically takes more time.⁸⁷⁸ It can also significantly contribute to *polarization* in society by amplifying extreme content, as such content typically incites more engagement.⁸⁷⁹ It also contributes to *misinformation*, as false claims about facts are often made to drive visitors and maximize surplus from OBA.⁸⁸⁰ In extreme cases, malicious actors can exploit OBA infrastructure with “bots” for their misinformation campaign, which can be destructive to society and democratic processes.

Furthermore, a systematic threat to the ability to be vulnerable in the online environment can have a chilling effect on freedom of expression. Some people

⁸⁷⁴ See Simone van der Hof et al., *The Child’s Right to Protection against Economic Exploitation in the Digital World*, 28 INT. J. CHILD. RIGHTS (2020). See in the context of video game interfaces and children’s rights Simone van der Hof et al., “Don’t Gamble With Children’s Rights”-How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment, 4 FRONT. DIGIT. HEALTH 822933 (2022).

⁸⁷⁵ G.A. Res. 44/25, Convention on the Rights of the Child (Nov. 20, 1989).

⁸⁷⁶ CFREU, *supra* note 43, Preamble.

⁸⁷⁷ See DUPR, *supra* note 674 at 157–160.

⁸⁷⁸ See CMA (UK) Study Online Platforms & Digital Advertising Final Report, *supra* note 33.

⁸⁷⁹ See Steve Rathje, Jay J. Van Bavel & Sander van der Linden, *Out-Group Animosity Drives Engagement on Social Media*, 118 PROC. NATL. ACAD. SCI. e2024292118 (2021).

⁸⁸⁰ Ledger of Harms, *supra* note 48; Ryan Mac Silverman Craig, *Facebook Has Been Showing Military Gear Ads Next To Insurrection Posts*, BUZZFEED NEWS (2021), <https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot> (last visited Apr 12, 2023).

“disconnect” or avoid engaging with digital services to avoid manipulative practices, taking away their contributions to public debate that increasingly occurs online.⁸⁸¹ Consumer manipulation via OBA can erode the capability of consumers to make authentic choices, which could later lead to difficulty in making such choices in the political realm. These effects pose a threat to individuals as a source of political power. This threat can be understood as an affront to human dignity, which acts as the concept providing humans “the power, and freedom, to choose how to shape their own time individually, and collectively, the power to construct boundaries between human time and non-human time, perhaps as well the duty to protect the time of mankind”.⁸⁸²

5.2.7.3 *Threat to Vulnerability*

Consumer manipulation can be understood as undermining human dignity “through thousand cuts” for individuals.⁸⁸³ Singled-out instances of OBA’s manipulative practices cause relatively small harm to individuals economically, psychologically, and physically when it comes to losing exact time.⁸⁸⁴ However, consumer manipulation harms are *numerous*.⁸⁸⁵ For example, exposure to a single dark pattern in a cookie banner can be a minor inconvenience, but being exposed to hundreds of such patterns can constitute a significant distraction and loss of time.⁸⁸⁶ This also works the other way—some companies, such as providers of platforms, may cause a small amount of harm to millions of people.⁸⁸⁷ This makes consumer manipulation a large-scale problem—from a societal perspective, aggregating the harm to everyone, the total harm is substantial.⁸⁸⁸

The harms of online manipulative practices, including in the context of OBA, are not fully quantifiable, what has historically been considered a threshold for tort law.⁸⁸⁹ For example, manipulative personalization and infinite scrolling increase the consumer’s time spent with digital services, but it is impossible to generalize precisely what harm this leads to in all cases. In essence, such manipulative

⁸⁸¹ Hong Tien Vu & Magdalena Saldaña, *Chillin’ Effects of Fake News: Changes in Practices Related to Accountability and Transparency in American Newsrooms Under the Influence of Misinformation and Accusations Against the News Media*, 98 JOURNAL. MASS COMMUN. Q. 769 (2021).

⁸⁸² See DUPR, *supra* note 674 at 152.

⁸⁸³ See Lingchi - Wikipedia, <https://en.wikipedia.org/wiki/Lingchi> (last visited Apr 12, 2023).

⁸⁸⁴ See Citron and Solove, *supra* note 625 at 816. See also COHEN, *supra* note 28.

⁸⁸⁵ Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. LAW REV. (2013), <https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/> (last visited Apr 12, 2023).

⁸⁸⁶ See generally Bart W. Schermer, Bart Custers & Simone van der Hof, *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*, 16 ETHICS INF. TECH. 171 (2014). See also Citron and Solove, *supra* note 625 at 816.

⁸⁸⁷ See Citron and Solove, *supra* note 625 at 816.

⁸⁸⁸ *Id.*

⁸⁸⁹ *Id.* at 817.

practices create an unmanageable *risk* of future harm related to any of the fundamental capabilities, starting from mental and physical well-being to economic participation.⁸⁹⁰ In the end, consumer manipulation via OBA leads to an online environment that is untrustworthy, that consumers cannot use without the increased threat that their vulnerability will be exploited and they will be made fragile.

In the EU law, human dignity can be understood as the right to have rights.⁸⁹¹ The capability approach enriches such understanding by contributing an ontological human vulnerability as the normative foundation of human dignity.⁸⁹² This thesis understands “human dignity” as the human capability, entitlement, and, to some extent, a right to be vulnerable in certain societal contexts. The human capability to be vulnerable enables people to be intimate, connect with others, reshape themselves, and build communities. In the context of OBA, respect for human dignity means giving human beings space to be vulnerable when receiving digital services without the continuous threat that their vulnerability will be observed, inferred, and exploited by providers of these services (or their customers).

The systemic threat that their vulnerabilities are exploited in the online environment can lead some consumers to have subjective experiences of insecurity, anxiety, and worthlessness. Yet, human dignity protects consumers beyond their subjective experiences and instead safeguards consumers as a group. Such an understanding of “consumer dignity” protects consumers from their interests in non-exploitation being subjected to the financial profit of the companies providing them with digital services whether or not they subjectively experience being harmed. In other words, consumer dignity can be said to be harmed when there is a clear and systematic asymmetry between the benefits and risks of the consumer and the shareholder – when the consumer takes the most risks while the shareholder takes the most benefit.

Lastly, threats of OBA to consumer dignity can be understood by focusing on the often involuntary and hidden risk-bearing by consumers in the online environment. An online environment that monetizes digital services via OBA infrastructure can be compared to gambling environments that are often designed to exploit consumer vulnerabilities.⁸⁹³ In gambling environments, people are aware of the context as entertainment, and they consciously choose to take associated risks. Online environments have become an inescapable part of daily life in a variety of societal contexts, including work, play, and social communication. By systematically exposing the consumers navigating these contexts to exploitative

⁸⁹⁰ See Solove and Citron, *supra* note 631.

⁸⁹¹ See DUPR, *supra* note 675 at 157.

⁸⁹² Luciano Floridi, *On Human Dignity and a Foundation for the Right to Privacy*, 29 PHILOS. TECHNOL. 307 (2016); Robeyns and Byskov, *supra* note 734; NUSSBAUM, *supra* note 635.

⁸⁹³ See generally SCHULL, *supra* note 496.

practices, digital service providers facilitating consumer manipulation via OBA take away their capability to be vulnerable within these contexts and harm their dignity.

5.3. Conclusion: Consumer Manipulation Harms of OBA

This section answers the fourth sub-question of the thesis:

SQ4: what are the harms of consumer manipulation via OBA?

Consumer manipulation via OBA undermines the consumer’s autonomy, and it may lead to seven types of harms: economic harms, environmental harms, affinity harms, privacy harms, authenticity harms, integrity harms, and dignity harms.

Economic harms include a direct economic loss to the consumer or structural harms through market failures, such as reduced innovation, reduced quality of content and services, increased prices, reduced welfare, and reduced trust in the market. *Environment harms* include adverse effects on the environment, such as increased carbon emission, battery overuse, an increase in waste, and adverse effects on animal welfare. *Affinity harms* include discrimination and oppression of specific (often marginalized) groups. *Privacy harms* include negative subjectives experiences for the consumer, such as emotional distress, disturbance, thwarted expectations, and anxiety. *Authenticity harms* entail the loss of “time of one’s own,” including loss of consortium, leisure, and earnings. *Integrity harms* include adverse effects on mental and physical health and fitness, including self-harm and loss of life. *Dignity harms* envisage systematic threats to individuals, groups of individuals, and core societal interests, such as democracy.

Lastly, Table 5-1 provides the list of consumer manipulation harms identified in this thesis, with some examples for each type of harm.

Table 5-1. Consumer manipulation harms of OBA

Harms		Examples
Economic harms (section 5.2.1)	<i>Economic loss: personal detriment</i> (section 5.2.1.1)	<ul style="list-style-type: none"> • consumer buys an unwanted product (e.g., a concert ticket) • consumer pays more than they otherwise would
	<i>Market harm: structural detriment</i> (section 5.2.1.2)	<ul style="list-style-type: none"> • reduction of consumer trust in online markets • investment in avoidance measures (e.g., adblockers) • emergence of the consumer exploitation market • inhibition of innovation • increased prices for advertised goods • poor returns to consumers

CHAPTER 5

Environment harms (section 5.2.2)		<ul style="list-style-type: none"> • increase in CO2 emissions • increase in electronic waste (killing device batteries) • increase in freshwater consumption • exploiting consumers' attachments to pets • facilitating illegal pet trade
Affinity harms (section 5.2.3)		<ul style="list-style-type: none"> • discrimination (e.g., targeting STEM jobs only to men) • oppression (e.g., targeting young LGBTQ+ consumers with "gay cure" advertisements)
Privacy harms (section 5.2.4)		<ul style="list-style-type: none"> • emotional distress (e.g., anxiety due to revealing mental health condition) • reputational harm (e.g., by disclosing sexual preference) • disturbance (e.g., due to intrusive or creepy ads)
Authenticity harms (section 5.2.5)		<ul style="list-style-type: none"> • loss of time (e.g., consortium, earnings, leisure)
Integrity harms (section 5.2.6)		<ul style="list-style-type: none"> • distorting self-image (e.g., Snapchat Dysmorphia) • encouraging self-harm
Dignity harms (section 5.2.7)	<i>to children</i> (section 5.2.7.1)	<ul style="list-style-type: none"> • systematic threat to children's integrity
	<i>to democracy</i> (section 5.2.7.2)	<ul style="list-style-type: none"> • disinformation • polarisation • lowering the quality of journalism
	<i>to vulnerability</i> (section 5.2.7.3)	<ul style="list-style-type: none"> • systematic threat to exploit vulnerabilities of online consumers

CHAPTER 6. BOUNDARIES OF CONSUMER MANIPULATION VIA OBA

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

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

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

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

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

⁸⁹⁶ See Johnny Ryan, *supra* note 55.

6.1. The EU Legal Framework for OBA

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

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

6.1.1. EU Consumer Protection Law

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⁹¹³ *Id.*, art 6(1)(a).

⁹¹⁴ *Id.* art. 6(1)(b)–(d).

⁹¹⁵ *Id.* art. 6(1)(e).

⁹¹⁶ *Id.* art. 6(1)(r).

⁹¹⁷ *Id.* rec. 19.

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

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

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

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

⁹²² *Id.* at 5.

⁹²³ *Id.* at 6.

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

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

To evaluate whether a practice is unfair and therefore prohibited by the UCPD, one must examine the practice in three steps, from the most specific to the most general prohibition. First, it needs to be established whether the practice is listed in Annex I as one of the blacklisted practices.⁹²⁹ In such a case, no further consideration is necessary, and the practice is prohibited. Second, if the practice is not listed in Annex I, it must be assessed whether the practice is either misleading (through actions⁹³⁰ or omissions⁹³¹) or aggressive,⁹³² including whether it exerts undue influence.⁹³³ In case such misleading or aggressive practices have or are likely to have an economic effect as described above, they can be found unfair and deemed prohibited. Third, as a last resort, when the first two situations don’t apply, the most general provision of the UCPD prohibits practices that are *otherwise*

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

⁹²⁵ *Id.* at art 5(2)(a)-(b). (emphasis added). Article 5(2)(b) states in full that “it materially distorts or is likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.” *Id.* art. 5(2)(b).

⁹²⁶ See *Id.* arts. 6–9.

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

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

⁹²⁹ *Id.* annex I.

⁹³⁰ *Id.* art. 6.

⁹³¹ *Id.* art. 7.

⁹³² *Id.* art. 8.

⁹³³ *Id.* art. 9.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⁹⁴¹ *Case C-646/22, Compass Banca Request, supra* note 434.

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

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

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

6.1.2. EU Personal Data Protection Law

Personal data protection legislation has been the hallmark of the EU response to prevent and mitigate harms stemming from the advance of information technologies that process personal data.⁹⁴⁵ The CFREU that included personal data protection as an individual fundamental right was proclaimed in 2000, shortly before Alphabet adopted OBA as a business model.⁹⁴⁶ Article 8 of the CFREU reiterates the EU approach to the processing of personal data, which, in essence, is only allowed in case there is sufficient legal ground provided by law, such as, for example, the consent of the person involved.⁹⁴⁷ The CFREU went into force in 2009, shortly after Facebook launched its advertising platform, including the controversial advertising *Beacon* that covertly tracked users over the Internet.⁹⁴⁸ The rise of social networks and OBA as the backbone of the online environment have largely triggered a call to update personal data protection rules, resulting in the adoption of the General Data Protection Regulation (GDPR), which entered into force on May 25, 2018.⁹⁴⁹

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

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

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

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

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

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

⁹⁴⁹ In the memorandum IP/10/63 from January 28, 2010, Commission calls for reform of the personal data protection rules. It starts by declaring that “Our privacy faces new challenges: behavioural advertising can use your internet history to better market products; social networking sites used by 41.7 million Europeans allow personal information like photos to be seen by others”. European Commission Press Release IP/10/63, The Commission, *supra* note 44. It also points to the Phorm’s predatory OBA in the UK as the concerning practice. Viviane Reding, the Commissioner, has also addressed this in her speech. Viviane Reding Member of the European Commission responsible for Information Society and Media Privacy: the challenges ahead for the European Union Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels, SPEECH/ 10/16 (Jan. 28, 2010), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_10_16.

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

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

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

⁹⁵¹ CHEN, *supra* note 947 at 94.

⁹⁵² Frederik J. Zuiderveen Borgesius, *Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, 32 *COMPUT. LAW SECUR. REV.* 256 (2016). *See* General Data Protection Regulation, *supra* note 44, rec. 30. (“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”)

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

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

⁹⁵⁵ *Id.*, art. 6 (f).

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

⁹⁵⁷ *Id.* at 5(3).

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

In order to avoid the proliferation of cookie banners in the online environment, the EU proposed the ePrivacy Regulation in 2017.⁹⁶⁰ The proposal included the requirement to centralize tracking decisions in browser settings that would allow consumers to choose how they wanted to be tracked over the Internet.⁹⁶¹ Such a rule allowed consumers to choose not to be tracked over the Internet and threatened the OBA industry with heavy financial losses. This regulation has been wholly stalled since the end of 2021.⁹⁶² This has given the OBA industry the time to continue exponential wealth-creation and to come up with a privacy-preserving versions of OBA while at the same time proliferating cookie banners in the online environment, most of which are manipulative.⁹⁶³

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

⁹⁵⁸ *Id.* at 2(d). (“‘communication’ means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.”)

⁹⁵⁹ *Id.* at 5(1).

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

⁹⁶¹ *Id.* recs. 23-25.

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

⁹⁶³ Most prominent project has been Google’s Privacy Sandbox that has intended to change OBA with technology that does not rely on cookies. Its use has continuously postponed, and now is considered to come into play in 2024 Chavez, *supra* note 245; The Privacy Sandbox: Technology for a More Private Web, PRIVACY SANDBOX, <https://privacysandbox.com/> (last visited Apr 23, 2023).

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

⁹⁶⁵ *Id.*, art. 5.

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

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

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

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

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

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

⁹⁶⁹ *Id.*

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

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

⁹⁷² *Id.* art. 5, 35.

⁹⁷³ *Id.* arts. 37-40.

⁹⁷⁴ *Id.* arts. 51-54.

⁹⁷⁵ *Id.* arts 57-59.

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

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

6.1.3. EU Competition Law

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

⁹⁷⁶ *Id.* arts. 83–89.

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

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

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

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

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

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

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

⁹⁸² *Id.* at 1.

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

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

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

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

⁹⁸⁷ *Id.* at 93.

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

⁹⁸⁹ *Id.* 44–46.

⁹⁹⁰ *Id.* at 48–56.

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

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

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

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

⁹⁹³ *Id.* at 368.

⁹⁹⁴ *Id.*

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

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

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

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

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

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

Spanish¹⁰⁰¹ competition authorities have conducted online advertising market studies finding that Alphabet dominates all search advertising and open exchange (AdTech) display markets.¹⁰⁰² Meta’s platforms hold a significant market share (40-50%) in the remaining display advertising market.¹⁰⁰³

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

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

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

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

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

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

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

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

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

¹⁰⁰⁸ *Id.*

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

¹⁰¹⁰ See Graef, *supra* note 46.

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

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

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

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

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

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

¹⁰¹⁴ *Id.*

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

¹⁰¹⁶ *Id.*

¹⁰¹⁷ See Natasha Lomas, *CJEU Ruling on Meta Referral Could Close the Chapter on Surveillance Capitalism*, TECHCRUNCH, Jul. 4, 2023, <https://techcrunch.com/2023/07/04/cjeu-meta-superprofiling-decision/> (last visited Jul 16, 2023). See Trevisan & Cuonzo - Caio Nunes, *CJEU Lands Groundbreaking Decision on Data Protection and Antitrust*, LEXOLOGY, Jul. 7, 2023, <https://www.lexology.com/library/detail.aspx?g=e722bd9d-5135-4536-90aa-5b58c4a268d7> (last visited Jul 16, 2023). See CJEU decision in Facebook proceeding: *Bundeskartellamt may take data protection rules into consideration*, BUNDESKARTELLAMT (2023), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/04_07_2023_Eu_GH.html (last visited Jul 16, 2023). See Foo Yun Chee, *Meta Loses as Top EU Court Backs Antitrust Regulators over Privacy Breach Checks*, REUTERS, Jul. 5, 2023, <https://www.reuters.com/technology/german-antitrust-watchdog-can-add-privacy-breaches-meta-probe-eu-court-says-2023-07-04/> (last visited Jul 16, 2023).

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

6.1.4. EU Digital Single Market¹⁰²¹

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

6.1.4.1 Before the DSA and the DMA

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

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

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

¹⁰²⁰ See *Id.*

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

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

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

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

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

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

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

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

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

¹⁰²⁸ *Id.* art. 9(1)(b).

¹⁰²⁹ *Id.* art. 6a.

¹⁰³⁰ *Id.* art. 28(b)(3).

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

the EU when they receive OBA-funded digital services and content without monetary payment. The P2BR aims to protect platform business customers and is a regulatory reaction to the European Commission finding Alphabet unfairly self-preferencing its services in the *Google Shopping* antitrust case 2017.¹⁰³² The P2BR sets out the rules for platforms (e.g., Google Shopping) to inform its business users (e.g., wanting to sell on Google Shopping) about the ranking criteria, including whether ranking is sponsored, whether personalization takes place, and whether it is based on consumer behavior.¹⁰³³ The P2BR attempts to address power asymmetries between platforms and smaller businesses, including in the context of paid ranking (which can be a form of OBA), by increasing transparency and fairness.¹⁰³⁴

6.1.4.2 *The DSA and the DMA*

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

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

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

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

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

¹⁰³⁵ Digital Services Act, *supra* note 2.

¹⁰³⁶ Digital Markets Act, *supra* note 14.

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

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

¹⁰³⁹ *Id.* rec. 13.

¹⁰⁴⁰ *Id.*

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

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

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

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

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

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

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

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

¹⁰⁴⁶ *Id.*

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

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

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

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

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

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

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

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

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

¹⁰⁵³ *Id.* art. 26.

¹⁰⁵⁴ *Id.* rec. 69.

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

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

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

¹⁰⁵⁵ *Id.* art. 26.

¹⁰⁵⁶ *Id.* art. 27.

¹⁰⁵⁷ *Id.* art. 39.

¹⁰⁵⁸ *Id.* art. 40.

¹⁰⁵⁹ *Id.* art. 46.

¹⁰⁶⁰ Digital Markets Act, *supra* note 14, art. 5(2).

¹⁰⁶¹ BKartA, Case VI-Kart 1/19 (V), Facebook (Ger.), *supra* note 1015.

¹⁰⁶² Digital Markets Act, *supra* note 14, rec. 36.

¹⁰⁶³ *Id.* at 5.

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

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

6.1.4.3 Artificial Intelligence Act (AIA)

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

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

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

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

¹⁰⁶⁵ AI Act Proposal, *supra* note 52.

¹⁰⁶⁶ *Id.* rec. 52.

¹⁰⁶⁷ *Id.* rec. 69.

¹⁰⁶⁸ *Id.* rec. 56.

¹⁰⁶⁹ *Id.* annex III.

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

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

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

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

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

¹⁰⁷² *Id.* art. 5(1)(a)-(b).

¹⁰⁷³ AI Act Mandates, *supra* note 367.

6.2. Prohibited OBA Practices

Academia,¹⁰⁷⁴ civil society,¹⁰⁷⁵ media,¹⁰⁷⁶ and politicians¹⁰⁷⁷ have called for an outright ban on OBA because it is fundamentally irreconcilable with democratic values and human rights. The *Tracking-Free Ads Coalition* has advanced this agenda in the European Parliament, which, in the discussions around the DSA, called for first prohibiting “micro-targeting” and starting a phase-out of OBA entirely, leading to its ultimate prohibition.¹⁰⁷⁸ The European Data Protection Supervisor (EDPS) also backed the European Parliament, inviting the European Commission to prohibit OBA via “pervasive tracking ultimately.”¹⁰⁷⁹

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

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

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

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

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

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

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

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

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

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

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

6.2.1. The Prohibition of OBA Using Special Categories of Data

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

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

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

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

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

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

¹⁰⁸⁶ See *Id.* art. 26(3), rec. 81.

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

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

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

¹⁰⁹⁰ See *Id.*, rec. 69.

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

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

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

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

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

¹⁰⁹³ *Id.* at 382.

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

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

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

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

¹⁰⁹⁸ *Id.*

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

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

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

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

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

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

¹¹⁰² *Id.*

¹¹⁰³ *Id.*

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

¹¹⁰⁵ See generally Klenk, *supra* note 305.

inference that consumers with “similar” mouse movements are more likely to click on the advertisement.¹¹⁰⁶

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

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

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

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

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

¹¹⁰⁸ Solove, *supra* note 631 at 4.

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

¹¹¹⁰ Solove criticizes “special categories of data” paradigm. See generally Solove, *supra* note 631.

¹¹¹¹ *Id.*

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

Another challenge with the Article 26(3) DSA is that the prohibition only applies to “online platforms”.¹¹¹² This means that other digital service providers are not explicitly prohibited from using special categories of data for their OBA practices. This may seem to be a loophole.¹¹¹³ It is likely that the regulator left this gap to relieve more minor actors from the regulatory burden. Such actors that are not “online platforms” include advertising intermediaries and other publishers (e.g., online newspapers). This gap is understandable if Article 26(3) DSA is read together with Article 46 DSA and Article 5 UCPD provisions. In particular, Article 46 DSA refers to “online advertising codes of conduct” that the European Commission is called to “encourage” the industry to commit to voluntarily.¹¹¹⁴ By establishing in codes of conduct (under Article 46 DSA) that OBA with special categories of data is prohibited, digital service providers that are not “online platforms” can be held liable under Article 5(2) UCPD to breach their “professional diligence” in case they process such data.¹¹¹⁵ Article 46 DSA codes of conduct will apply from 18 August 2025.¹¹¹⁶

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

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

¹¹¹³ See generally Hacker, *supra* note 54.

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

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

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

6.2.2. The Prohibition of OBA for Minors

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

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

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

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

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

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

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

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

¹¹²³ *Id.*, art. 28(2).

¹¹²⁴ *Id.*, art. 26(3).

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

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

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

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

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

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

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

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

¹¹³⁰ See Dumitrascu, *supra* note 1129.

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

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

¹¹³³ See Dumitrascu, *supra* note 1129.

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

6.2.3. The Prohibition of Profiling with Significant Effects

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

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

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

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

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

¹¹³⁷ *Id.*, art 22.

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

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

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

sees an advertisement can be considered a “decision” within the meaning of Article 22 GDPR, and secondly, even if it does, whether such a decision produces legal or similarly significant effects.¹¹⁴¹ In 2021, the Amsterdam District Court ruled in the so-called “Uber ADM Case” that algorithmic matching of the drivers and consumers did not constitute automated decision-making because the interests of drivers and consumers were not “significantly” affected.¹¹⁴² Also, in 2021, the so-called “Schufa Case” was referred to the CJEU to decide whether using a particular credit scoring system constitutes automated decision-making under Article 22 GDPR.¹¹⁴³ The final judgment in the Schufa case is expected in late 2023.¹¹⁴⁴ While this can clarify the scope of Article 22 GDPR, its application to OBA will likely remain provisional.

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

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

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

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

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

¹¹⁴⁴ Andreas Hauselmann, *supra* note 1140.

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

¹¹⁴⁶ *Id.*

¹¹⁴⁷ *Id.*

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

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

6.2.4. The Prohibition of Unfair Practices and OBA

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

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

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

¹¹⁵⁰ *Id.*, art. 9(2).

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

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

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

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

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

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

¹¹⁵⁷ *Id.*, an. I, art. 11.

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

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

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

¹¹⁵⁸ *Id.*, art. 7.

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

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

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

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

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

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

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

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

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

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

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

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

¹¹⁶⁷ *Id.*, art. 9(c).

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

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

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

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

¹¹⁷² *Id.* 246.

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

¹¹⁷⁴ See *Id.*, art. 5(2).

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

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

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

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

¹¹⁷⁵ GALLI, *supra* note 41, 248.

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

¹¹⁷⁷ See Hacker, *supra* note 54, 12.

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

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

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

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

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

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

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

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

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

¹¹⁸⁵ *Id.*, art. 5(3), rec.19.

¹¹⁸⁶ *Id.*, art. 5(3), rec.19.

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

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

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

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

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

Thirdly, and lastly, Article 1 UCPD clarifies that the UCPD only protects against economic harms.¹¹⁹³ Typically, the UCPD does not safeguard against health, safety, affinity, or environmental harms of business-to-consumer (B2C) commercial practices.¹¹⁹⁴ However, the CJEU has clarified that the UCPD safeguards other interests in case they are in conjunction with the consumer’s economic interest.¹¹⁹⁵ This “economic” aspect of the UCPD was considered a limiting factor in enforcing consumer protection rules for OBA, as some argued that economic exchange was absent in OBA contracts.¹¹⁹⁶ Over time, consumer protection authorities, such as those in Germany¹¹⁹⁷ and Italy,¹¹⁹⁸ have clarified that consumer protection rules

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

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

¹¹⁹² Case C-646/22, *Compass Banca* Request, *supra* note 434.

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

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

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

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

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

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

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

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

6.2.5. The Proposed Prohibitions of Manipulation via AI

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

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

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

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

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

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

CHAPTER 6

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

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

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

¹²⁰² *Id.*

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

¹²⁰⁴ *Id.* art. 5(1)(b).

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

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

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

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

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

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

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

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

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

¹²⁰⁸ *Id.*

¹²⁰⁹ *Id.*

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

6.3. Legal Grounds for OBA

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

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

6.3.1. Consent

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

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

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

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

¹²¹³ See Zuiderveen Borgesius, *supra* note 1212.

6.3.1.1 *Conditions*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

¹²²⁸ See Schermer, Custers, and van der Hof, *supra* note 88, 5.

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

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

¹²³¹ *Id.*

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

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

Fourthly, consent has to be *freely given* and, therefore, an expression of a consumer’s genuine desire.¹²³⁷ Digital service providers have to ensure that the decision-making of the consumer is free of coercive and manipulative influences.¹²³⁸ Article 7 GPDR lists two such elements to consider when evaluating if consent is freely given – (a) whether publishers provide alternative options¹²³⁹ and (b) whether there is an “imbalance” between parties.¹²⁴⁰ These two elements can help evaluate the legitimacy of the OBA industry’s consent practices.

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

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

¹²³⁴ See *Id.*, at 7.

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

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

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

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

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

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

¹²⁴¹ See *Id.*, at 67.

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

¹²⁴³ See *Id.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3.1.2 Consent in AdTech

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

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

¹²⁵² *Id.*

¹²⁵³ *Id.*

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

¹²⁵⁵ *Id.*

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

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

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

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

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

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

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

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

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

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

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

In September 2022, upon appeal of the IAB Europe, the Belgian DPA referred the case to the CJEU, requesting a preliminary ruling on this matter.¹²⁶⁵ While the CJEU judgment is not expected until 2024, the Belgian DPA requested IAB Europe to comply with the decision from July 11, 2023.¹²⁶⁶ As a response, on 16 May 2023, IAB Europe introduced TCF 2.2., which includes new rules for TCF participants.¹²⁶⁷ TCF 2.2. requires that the legal basis for OBA is consent from each of the “vendors”. It seems that TCF 2.2. will significantly decrease the number of vendors publishers can allow to track their consumers. It also requires publishers to show the number of vendors on the first layer of banners where consumers can accept placing third-party cookies for OBA.

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

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

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

¹²⁶⁴ *Id.*

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

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

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

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

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

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

6.3.1.3 *OBA Contracts*

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

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

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

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

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

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

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

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

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

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

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

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

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

¹²⁷⁷ *See Id.*

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

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

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

¹²⁸¹ *See Id.*, at 2.

¹²⁸² *See Id.*, at 10.

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

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

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

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

6.3.2. Contractual Necessity

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

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

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

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

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

¹²⁸⁹ *Id.* at 35.

¹²⁹⁰ *Id.*

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

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

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

¹²⁹⁴ See *Id.*

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

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

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

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

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

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

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

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

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

¹³⁰¹ *Id.*

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

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

6.3.3. Legitimate Interest

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

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

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

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

¹³⁰⁵ *Id.* at 106.

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

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

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

¹³⁰⁹ *Id.*

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

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

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

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

¹³¹¹ CHEN, *supra* note 947 at 2.

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

¹³¹³ *Id.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.4. OBA Transparency & Fairness

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

6.4.1. Information Disclosure

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

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

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

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

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

¹³³² *Id.*, art. 26(1)(a).

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

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

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

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

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

¹³³⁴ *Id.*, art. 44.

¹³³⁵ *Id.*, art. 26(1)(b).

¹³³⁶ *Id.*, art. 26(1)(c).

¹³³⁷ *Id.*, art. 26(1)(d).

¹³³⁸ *Id.*, art. 68.

¹³³⁹ *Id.*

¹³⁴⁰ *Id.*, art. 26(1)(d).

¹³⁴¹ e.g., disclosure of profiling can be as limited as: “*To predict which ads you might like, we also consider your ad preferences, activity and other factors.*” It is doubtful that such note can amount to “meaningful” disclosure.

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

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

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

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

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

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

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

¹³⁴⁵ *Id.*

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

¹³⁴⁷ *Id.*

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

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

6.4.2. OBA Scrutiny: Archives, Access, Audit

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

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

¹³⁴⁹ *Id.*, art 44 (h).

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

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

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

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

Academia has long been concerned about the potential harms of OBA, practices of which have been challenging to scrutinize.¹³⁵⁵ In response to the Cambridge Analytica scandal, Alphabet¹³⁵⁶ and Meta¹³⁵⁷ have provided advertising repositories since 2018.¹³⁵⁸ These early forms of advertising repositories had a variety of shortcomings; for example, they were limited to political advertising and did not offer information regarding the targeting criteria used.¹³⁵⁹ In August 2023, Alphabet and Meta updated repositories to comply with Article 39 DSA, making all advertisements shown on their platforms available to the public.¹³⁶⁰ Neither of these repositories entails disclosing criteria for behavioral personalization (e.g., predicted interests), and it seems that Meta does not even disclose if behavioral personalization occurs.¹³⁶¹

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

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

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

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

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

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

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

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

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

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

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

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

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

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

¹³⁶² See Hacker, *supra* note 54.

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

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

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

¹³⁶⁶ *Id.*, art. 4.

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

¹³⁶⁸ *Id.*, rec. 72.

¹³⁶⁹ *Id.*, rec. 72.

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

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

6.4.3. Managing OBA Risks

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

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

¹³⁷⁰ *Id.*, art. 15 (1).

¹³⁷¹ *Id.*, art. 15 (3).

¹³⁷² Digital Services Act, *supra* note 2, art. 37.

¹³⁷³ *Id.*, art. 34 (1).

¹³⁷⁴ *Id.*, art. 34 (1) (b).

¹³⁷⁵ *Id.*, art. 34 (2).

¹³⁷⁶ *Id.*, rec. 84.

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

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

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

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

¹³⁷⁷ *Id.*, rec. 81.

¹³⁷⁸ *Id.*, art. 35.

¹³⁷⁹ *Id.*, art. 35.

¹³⁸⁰ Digital Markets Act, *supra* note 14, rec. 14.

¹³⁸¹ See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 100.

¹³⁸² *Id.* at 98.

¹³⁸³ *Id.*, art. 35(1)(i).

¹³⁸⁴ See European Parliament Study Consent in Targeted & Behavioral Advertising, *supra* note 36 at 98.

¹³⁸⁵ *Id.*

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

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

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

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

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

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

¹³⁸⁸ *Id.*, rec. 81.

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

¹³⁹⁰ *Id.*

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

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

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

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

¹³⁹² *Id.*

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

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

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

¹³⁹⁶ See Hacker, *supra* note 54.

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

BOUNDARIES OF CONSUMER MANIPULATION VIA OBA

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

6.5. Conclusion: Boundaries of Consumer Manipulation via OBA

This section answers SQ5 of this thesis:

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

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

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

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

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

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

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

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

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

¹³⁹⁹ *Id.*, art 28 (3).

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

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

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

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

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

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

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

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

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

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

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

CHAPTER 7. CONCLUSIONS: THE ENDS OF OBA

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

7.1. Conclusion

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

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

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

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

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

¹⁴⁰⁷ See Boerman, Kruijkemeier, and Zuiderveen Borgesius, *supra* note 81, at 364.

¹⁴⁰⁸ See Zard and Sears, *supra* note 1, at 800.

¹⁴⁰⁹ See ZUIDERVEEN BORGESIOUS, *supra* note 25, at 35–38.

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

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

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

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

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

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

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

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

¹⁴¹⁵ See Veale and Zuiderveen Borgesius, *supra* note 31.

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

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

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

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

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

¹⁴¹⁷ European Commission Study Dark Patterns & Manipulative Personalization, *supra* note 53.

¹⁴¹⁸ See e.g., Leiser, *supra* note 466.

¹⁴¹⁹ See Strycharz and Duivenvoorde, *supra* note 361 at 7.

¹⁴²⁰ See GALLI, *supra* note 41.

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

¹⁴²² See generally Hartmann et al., *supra* note 797. See generally Pärssinen et al., *supra* note 797.

¹⁴²³ Wachter, *supra* note 80.

privacy harms include emotional distress, disturbance, thwarted expectations, and anxiety.¹⁴²⁴

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

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

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

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

¹⁴²⁴ See Citron and Solove, *supra* note 625 at 841.

¹⁴²⁵ See generally Sunstein, *supra* note 831.

¹⁴²⁶ See Franklin et al., *supra* note 39. Molly Russell inquest, *supra* note 39.

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

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

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

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

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

¹⁴²⁷ See Guidance on the Interpretation of the Unfair Commercial Practices Directive, *supra* note 1155 at 1.1.1.

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

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

7.2. Recommendations

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

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

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

¹⁴²⁸ See Shields, *supra* note 176.

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

Two of the most pressing cases for consumer manipulation via OBA are directly related to Alphabet and Meta. Firstly, the European Commission is considering forcing Alphabet to divest parts of its business due to its potential abuse of its dominant position in the AdTech market of OBA.¹⁴³⁰ Secondly, since the GDPR entered into force, Meta has engaged in a “catch-me-if-you-can” race against asking consumers for their consent for OBA under Article 6 (1) GDPR.¹⁴³¹ The European Data Protection Board’s (EDPB) binding decision of October 27, 2023, suggests that Meta’s OBA practices have been illegitimate between 2018 and 2023.¹⁴³² With this in mind, the OBA practices of these companies must be closely investigated, including compliance with Article 35 DSA measures regarding risk mitigation.

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

The DSA and the DMA require Alphabet and Meta to submit risk assessments and audit reports, including with regard to their profiling practices. The European Commission will receive the latest auditing reports (for profiling techniques) in March 2024.¹⁴³⁷ Therefore, it is reasonable that the European Commission starts a formal investigation only after reviewing the first wave of reports provided by these companies. In order to adequately evaluate the OBA practices of the gatekeepers,

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

¹⁴³¹ Datatilsnet (No.) (Jul. 14, 2023), *supra* note 1308.

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

¹⁴³³ Digital Services Act, *supra* note 2, 56 (2).

¹⁴³⁴ *Id.*, art. 51.

¹⁴³⁵ Digital Markets Act, *supra* note 14, art. 23.

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

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

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

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

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

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

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

¹⁴³⁸ See *European Centre for Algorithmic Transparency*, EUROPEAN COMMISSION (2023), https://algorithmic-transparency.ec.europa.eu/index_en (last visited Oct 26, 2023).

¹⁴³⁹ Morel et al., *supra* note 546.

¹⁴⁴⁰ Digital Services Act, *supra* note 2, 26 (3).

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

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

¹⁴⁴¹ ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 123 at 29.

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

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

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

7.3. Going Forward

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

Digital technologies and markets are evolving fast. Gatekeepers now deploy generative AI applications, such as Microsoft 365 Copilot,¹⁴⁴⁵ and extended reality (xR) devices, such as Apple Vision Pro¹⁴⁴⁶ and Meta Quest,¹⁴⁴⁷ to fundamentally change the way digital technologies mediate human experience in all aspects of individuals’ daily lives. Regardless of the plethora of threats associated with these technologies, the central challenge with them, as with OBA, is this economic logic and the asymmetrical relationship between consumers and companies that provide

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

¹⁴⁴⁴ See ZUBOFF, *supra* note 20. See also COHEN, *supra* note 28.

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

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

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

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

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

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

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

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

¹⁴⁴⁹ See Kai Zenner, *Fixing the GDPR: Towards Version 2.0*, DIGITIZING EUROPE (2021), https://www.kaizenner.eu/post/gdpr_vol2 (last visited Oct 26, 2023).

¹⁴⁵⁰ See DE GREGORIO, *supra* note 154 at 2.

¹⁴⁵¹ See DUPR, *supra* note 674.

¹⁴⁵² See *Id.*

¹⁴⁵³ See ZUBOFF, *supra* note 20.

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

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

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

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

EPILOGUE

The title of this thesis, “Power & Dignity,” refers to the two often implicit goals within the European Union’s (EU) digital policy, including in the context of online behavioral advertising (OBA). Sometimes, these two goals are expressed as the objectives of the internal market and fundamental rights, market efficiency and consumer autonomy, welfare and fairness, entrepreneurial freedom and societal justice, profit maximization, and consumer privacy. In essence, *power* refers to the liberal imperative of individuals, groups, markets, and states to increase their political and economic capabilities or freedom. On the other hand, *dignity* refers to the European conception of both the source and the boundary of such freedom.

The emergence of OBA as the central business model of a thriving digital economy and the EU regulatory response to protect consumers’ (including their human rights) interests illustrates the seemingly conflicting “ends” of the OBA industry and the EU regulator. The subtitle of the thesis: “The Ends of OBA in the EU,” not only refers to the dual objectives of power and dignity but also to the *recurring* perception that an era in which the OBA is the central business model of the digital economy, is coming to an end.

The final resolution of this dichotomy and setting the boundaries for exploitation in the digital markets is a question of the political economy. An elegant resolution would require an industrial policy that makes *power* interests contingent on *dignity* interests and rewards the industry actors that find solutions to increase welfare and efficiency without consumer exploitation and earn economic profit without infringing consumer privacy. In other words, in the just digital markets, there can be no gains in welfare, efficiency, shareholder value, and market power without respect for “consumer dignity”.

Finally, just or unjust, all human conflicts are resolved in our shared *joy* of life:¹⁴⁵⁶

O Freunde, nicht diese Töne!
Sondern lasst uns angenehmere anstimmen
Und freudenvollere!
Freude!
Freude!

¹⁴⁵⁶ Beethoven, Ludwig van (1980). Ode to joy: from Symphony no. 9. Chicago Symphony Orchestra [2015]

ACKNOWLEDGMENTS

Francien Dechesne found me outside the *Kamerlingh Onnes Building* when I was looking for a purpose, and she took me in as her research assistant. She believed in me, stood by me, taught me to value authenticity and excellence, and encouraged me to define and pursue my purpose. In doing so, she has had a significant mark on my life, for which I will always be grateful. I am also profoundly thankful to Bart Custers and Simone van der Hof. They have always moved me forward and protected me from myself when needed. They have enabled me with time and resources and taught me patience and humility. I am lucky to have had them as supervisors.

eLaw – *Center for Law and Digital Technologies* has been the closest thing I had to a family for the past seven years. I am thankful to everyone there for warmly welcoming me and creating an ideal environment for me to work in.

I am grateful to Bart Schermer for giving me the first-ever lecture about the Internet, taking charge of my Ph.D. committee, and teaching me that academic excellence and joy go together. I am grateful to many others whose mentorship and intellectual friendship have shaped me as a researcher, teacher, and human being. I thank Gianclaudio Malgieri, Mark Leiser, Andreas Häuselmann, and Alan Sears for helping me purify and strengthen my ideas. I am grateful to Eduard-Fosch Villaronga for teaching me how things get done (“pam-pam”) and sending me to Berlin for the Axel Springer Award ceremony. Eduard, winning the prize with you and traveling to Italy are wonderful memories.

Many people have contributed to this thesis by discussing my ideas at conferences, workshops, and seminars. I am particularly grateful for the rare individuals who have carefully read and commented on the earlier drafts of the thesis. Daniel Susser, Marijn Sax, Christiana Santos, and Egelyn Braun gave me invaluable feedback and helped me resolve complex conceptual challenges. Some others have contributed to my thesis by their participation in discussions: Luciano Floridi, Brett Frischmann, Paul Nemitz, Mireille Hildebrandt, Marco Blocher, and Sandra Wachter have shaped my ideas by participating in the events I organized regarding my thesis.

Shoshana Zuboff has a particular imprint on the research underlying this thesis. In 2019, Francien handed me “*The Age of Surveillance Capitalism*,” which gave me a quantum leap. I see my first reading of this book as a personal (*2001: Space Odyssey*) black monolith moment, and it is a great honor that Prof. Zuboff is a member of my Ph.D. committee. I am also profoundly grateful that Frederik Zuiderveen Borgesius and Vanessa Mak, scholars I deeply respect and admire, also decided to join the committee. I could not have asked for a more ideal committee.

Some of my most cherished memories I made while writing this thesis were at the Oxford Internet Institute (OII) Summer Doctoral Program (SDP). I am so lucky to have met peers who mastered their fields and skillfully warmed my heart to their various beautiful perspectives. I am grateful to Simone van der Hof and Leiden law

ACKNOWLEDGMENTS

faculty for funding this experience and to the OII staff, especially Gemma Newlands and Vicky Nash, for helping us create this fantastic network.

Like everything in life, this thesis is not a product of an entirely solitary quest. We are entwined with the people in our lives, and many friends from Leiden and Oxford helped me move forward with various tasks. Thomas Rijntalder helped me with the *samenvatting* (the Dutch summary). Charlotte Spencer-Smith, Mora Matassi, Assia Wirth, Soumya Patnaik, and Seif Kabil proofread parts of my thesis. Dejan Tatic and Karolina Alama gave me valuable feedback. While *Borgman & Borgman* and *Bar Lokaal* provided me with quality coffee, friends at *Sporting Leiden* helped me find flow on many cold Sundays.

My family in Georgia gave me the fuel I needed to complete this thesis. My father opened my eyes to the future, my mother believed in me, and my brother taught me not to back down. My boys, with whom I grew up in the streets of Tbilisi, have taught me to fight for freedom and justice. The belief that my work contributes to a more just world that brings my family and friends a bit more joy was the idea that kept me going in the darkest of moments.

Lastly, I am grateful to my muse. Agata, you make everything beautiful. Having you close while working on this thesis marks the most idyllic time of my life.

BIBLIOGRAPHY

BIBLIOGRAPHY

Law

European Union (EU) Primary Law

- Charter of Fundamental Rights of The European Union, Oct. 26, 2012, O.J. (C 326) 391.*
- Consolidated Version of the Treaty Establishing the European Community, Dec. 24, 2002, O.J. (C 325).*
- Consolidated Version of the Treaty of the European Union, Oct. 26, 2012, O.J. (C 326) 15.*
- Consolidated Version of the Treaty on the Functioning of the European Union, Jun. 7, 2016 O.J. (C 2012) 47.*
- Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007 O.J. (C 306).*
- Treaty of Rome Establishing the European Economic Community, Mar. 25, 1957.*

EU Secondary Law

- Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) O.J. 2002 (L 201) 31.*
- Directive (EC) 2005/29 of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') O.J. 2005 (L 149) 22.*
- Directive (EEC) 93/13 of the Council of 5 April 1993 on Unfair Terms in Consumer Contracts, O.J. 1993 (L 95) 29.*
- Directive (EU) 2010/13 of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) 2010 O.J. (L 95).*
- Directive (EU) 2011/83 of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, Amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council O.J. 2011 (L 304).*
- Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities O.J. 2018 (L 303).*
- Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 Amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC*

BIBLIOGRAPHY

- and 2011/83/EU of the European Parliament and of the Council as Regards the Better Enforcement and Modernisation of Union Consumer Protection Rules, O.J. 2019 (L 328) 7.*
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services O.J. (L 136) 1.*
- Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive 2009/22/EC (Text with EEA Relevance) O.J. 2020 (L 409).*
- Regulation (EC) 2004/139 of 20 January 2004 on the Control of Concentrations between Undertakings (the EC Merger Regulation) (Text with EEA Relevance) O.J. 2004 (L 24).*
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) O.J. 2016 (L 119).*
- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services, 2019 O.J. (L 186) 57.*
- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) O.J. 2022 (L 265) 1.*
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance). O.J. 2022 (L 277).*

Council of Europe (CoE)

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

United Nations (UN)

- G.A. Res. 217 (III)A, Universal Declaration of Human Rights (Dec. 10, 1948).*
- G.A. Res. 2200 (XXI)A, International Covenant on Civil and Political Rights (Dec. 16, 1966).*
- G.A. Res. 2200 (XXI)A, International Covenant on Economic, Social & Cultural Rights (Dec. 16, 1966).*
- G.A. Res. 44/25, Convention on the Rights of the Child (Nov. 20, 1989)*

Germany

Grundgesets[GG][Basic Law], translation at: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html (accessed October 31, 2023).

BIBLIOGRAPHY

Case Law

Court of Justice of the European Union (CJEU)

- Case C-54/99, *Église de Scientologie*, 14 March 2000, ECLI:EU:C:2000:124.
Case C-628/17, *Orange Polska*, 12 June 2019 ECLI:EU:C:2019:480.
Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801.
Case C-371/20, *Peek & Cloppenburg*, 2 September 2021, ECLI:EU:C:2021:674.
Case C-184/20, *Vyriausioji tarnybinės etikos komisija*, August 1, 2022, ECLI:EU:C:2022:601.
Case T-190/10, *Egan & Hackett v. Parliament*, 28 March 2012, ECLI:EU:T:2012:165.
Case C-252/21, *Meta Platforms and Others*, July 4, 2023, ECLI:EU:C:2023:537.
Case C-36/02, *Omega*, 14 October 2004, ECLI:EU:C:2004:614.
Case C-540/08, *Mediaprint Zeitungs- und Zeitschriftenverlag*, October 9, 2010. ECLI:EU:C:2010:660.
Case C-210/96, *Gut Springenheide & Tusky v. Oberkreisdirektor des Kreises Steinfurt*, 16 July 1998, ECLI:EU:C:1998:369.
Case 85/76, *Hoffmann-La Roche v. Commission*, 13 February 1979, ECLI:EU:C:1979:36.
Case C-634/21, *Schufa Holding and Others (Scoring)*, Request for a preliminary ruling, 2021.
Case C-646/22, *Compass Banca*. Request for a preliminary ruling, 2022.

European Court of Human Rights (ECtHR)

- Benedik v. Slovenia*, no. 62357/14 (ECHR, 24 April 2018).
Perry v. United Kingdom, no 63737/00, ECHR 2003-IX.
Vinter and Others v. the United Kingdom [GC], nos. 66069/09, 130/10 and 3896/10, ECHR 2013.

Germany

- Bundesgerichtshof [BGH][Federal Court of Justice] Jun. 23, 2020, (Bundeskartellamt v. Facebook) Case LVR 69/19, ECLI:DE:BGH:2020:230620BKVR69.19.0 (Ger.)
translation at: <https://doi-org.ezproxy.leidenuniv.nl/10.1007/s40319-020-00991-2>.
Bundesverfassungsgericht [BVerfG][Federal Constitutional Court] Dec. 15, 1983, (self-determination) 1 BvR 209/83, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983 (Ger.)
translation at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
Kammergericht Berlin [KG][Higher Court of Berlin] Jan. 24, 2014, 5 U 42/12 (Ger.)
Landgericht Berlin [LB] [Regional Court of Berlin] Apr. 30, 2013, 15 O 92/12 (Ger.).

Italy

The Netherlands

- Hof Amsterdam, 4 April 2023, JAR 2023, m.nt CM Jakimowicz (*Uber chauffeurs v. Uber*)
ECLI:NL:GHAMS:2023:796 (Neth.) [Uber ADM]

BIBLIOGRAPHY

Policy Documents

EU Law Proposals

- Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM (2017) 10 [Proposal for ePrivacy Regulation].*
- Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 Final (Apr. 21, 2021) [Proposal for Artificial Intelligence Act].*
- Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising, COM (2021) 731.*

European Commission Antitrust Decisions

- Commission Decision of 3 November 2008, Case No Comp/M4731 *Google/DoubleClick*, C (2008) 927.
- Commission Decision of 27 June 2017, Case AT.39740 *Google Search (Shopping)*, C (2017) 4444.
- Commission Decision of 7 July 2018, Case At.40099 *Google Android*, C (2018) 4761.
- Commission Decision of 20 March 2019, Case AT. 40411 *Google Search (AdSense)*, C (2019) 2173.

Other EU Policy Documents

- Amendments Adopted by the European Parliament on 20 January 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM(2020)0825 – C9-0418/2020 – 2020/0361(COD), P9_TA(2022)0014, O.J. 2022 (C336) 48. https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html (Accessed November 16, 2022).*
- Amendments by the European Parliament and Council on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD), June 20, 2023 Draft. <https://artificialintelligenceact.eu/wp-content/uploads/2023/08/AI-Mandates-20-June-2023.pdf> (Accessed October 31, 2023).*
- Article 29 Data Protection Working Party (2010) “Opinion 2/2010 on Online Behavioral Advertising.”
- Article 29 Data Protection Working Party (2011) “Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising.”
- Article 29 Data Protection Working Party (2013) “Opinion 02/2013 on Apps on Smart Devices.”
- Article 29 Data Protection Working Party (2014) “Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC.”
- Article 29 Data Protection Working Party (2016) “Cookie Sweep Combined Analysis – Report.”

BIBLIOGRAPHY

- Article 29 Data Protection Working Party (2017) “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679.”
- Article 29 Data Protection Working Party (2018) “Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679.”
- Article 29 Data Protection Working Party (2018). “Guidelines on Consent Under Regulation 2016/679.
- Commission Notice, Guidance on Ranking Transparency Pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, O.J. 2020 (C 424)*
- Commission Notice, Guidance on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market (Text with EEA Relevance). 2021 C (526) 01.*
- Commission Notice, Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, O.J. 2019 (C 323) 04.*
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of the Regions, 2030 Digital Compass: The European Way for the Digital Decade, 2021 COM (2021) 118.*
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and Committee of the Regions, A Digital Single Market Strategy for Europe, COM (2015) 192. 2015.*
- European Commission (2015), *Study on the Welfare of Dogs and Cats Involved in Commercial Practices – Final Report*. Specific Contract SANCO 2013/12364. https://food.ec.europa.eu/system/files/2016-10/aw_eu-strategy_study_dogs-cats-commercial-practices_en.pdf.
- European Commission Press Release. “Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google and Meta, in Online Display Advertising” 11 March 2022, IP/22/1703, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1703 (Accessed October 31, 2023).
- European Commission Press Release. “Commission Opens Investigation Into Possible Anticompetitive Conduct by Google and Meta, in Online Display Advertising,” 11 March 2022, IP/22/1703. https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1703.
- European Commission Press Release. “Commission Sends Statement of Objections to Google,” 14 June 2023, IP/23/3207, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207. (Accessed October 31, 2023)
- European Commission Press Release. “Commission sends Statement of Objections to Meta over abusive practices benefiting Facebook Marketplace,” 19 December 2022, IP/22/7728 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7728 (Accessed October 31, 2022)
- European Commission Press Release. “Consumer Scoreboard.” 27 March 2023. IP/22/1703. Accessed March 30, 2023. https://ec.europa.eu/commission/presscorner/detail/e/ip_23_1891.
- European Commission Press Release. “Digital Markets Act: Commission Designates Six Gatekeepers.” 6 September 2023, IP/23/4328. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328. (Accessed November 2, 2023).

BIBLIOGRAPHY

- European Commission Press Release. “DSA: Very Large Online Platforms and Search Engines.” April 25, 2023, IP/23/2413. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.
- European Commission Press Release. “Europeans’ Privacy Will Be Big Challenge in next Decade, Says EU Commissioner” 28 January 2010, IP/10/63 https://ec.europa.eu/commission/presscorner/detail/en/IP_10_63 (Accessed October 31, 2023).
- European Commission Press Release. “Manipulative Online Practices.” 30 January 2023, IP/23/418 Accessed March 2, 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.
- European Commission Speech 01/340, “The Future for Competition Policy in the European Union.” Mario Monti, July 9, 2001. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_01_340/SPEECH_01_340_EN.pdf (accessed November 2, 2023).
- European Commission Speech 10/16, “Viviane Reding Member of the European Commission Responsible for Information Society and Media Privacy: The Challenges Ahead for the European Union Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels,” January 28, 2010. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_10_16. (Acc. Oct. 31)
- European Commission Speech 19/6251, “Laudatio Speech for Axel Springer Award winner Shoshana Zuboff by President-elect Dr. Ursula von der Leyen,” November 10, 2019. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_19_6251/SPEECH_19_6251_EN.pdf (Acc. Oct. 31).
- European Commission Speech 23/3288, “Remarks by Executive Vice-President Vestager.” June 14, 2023. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_3288. Accessed November 2, 2023.
- European Commission, Commissioner Thierry Breton Statement. “Here Are the First 7 Potential ‘Gatekeepers’ under the DMA.” 4 July 2023, S/23/3674 https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_3674. Accessed July (Accessed November 2, 2023).
- European Commission, Consumers, Health, Agriculture and Food Executive Agency (2018) *Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union – Final Report*, Publications Office of the European Union, <https://data.europa.eu/doi/10.2818/990439> (Acc. Oct. 31).
- European Commission, Directorate-General for Communications Networks, Content and Technology (2023) *Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers, and Advertisers – Final Report*, Publications Office of the European Union, <https://data.europa.eu/doi/10.2759/294673> (Acc. Oct. 31).
- European Commission, Directorate-General for Justice (2010) *2010 Annual Report from the Commission on the Application of the EU Charter of Fundamental Rights*, Publications Office, 2011, <https://data.europa.eu/doi/10.2775/179>.
- European Commission, Directorate-General for Justice and Consumers (2017) *Study on Measuring Consumer Detriment in the European Union – Final Report, Part 1: Main Report*. Publications Office of the European Union, <https://data.europa.eu/doi/10.2818/87261> (Acc. Oct. 31).
- European Commission, Directorate-General for Justice and Consumers (2022) *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns*

BIBLIOGRAPHY

- and Manipulative Personalisation – Final Report.*” Publications Office of the European Union, <https://data.europa.eu/doi/10.2838/859030>.
- European Data Protection Board (2019) “Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects.”
- European Data Protection Board (2020) “Guidelines 05/2020 on Consent under Regulation 2016/679.”
- European Data Protection Board (2021) “Guidelines 8/2020 on the targeting of social media users.”
- European Data Protection Board (2022) “Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognize and avoid them.”
- European Data Protection Board Press Release. “The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC.” 21 January 2019. https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Accessed November 2, 2023.
- European Data Protection Board Press Release. “EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta”, 1 November 2023. https://edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en. Accessed November 2, 2023.
- European Data Protection Supervisor (2017). “Opinion 1/2021 On the Proposal For A Digital Services Act.”
- European Parliament Press Release. “Digital: EU Must Set the Standards for Regulating Online Platforms, Say MEPs.” October 20, 2020, 20201016IPR89543. <https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps>.
- European Parliament Resolution of 18 June 2020 on Competition Policy, 2021 O.J. (C 362) 22.*
- European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies (2021a) *Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users’ Informed Consent*, Study PE 694.680, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU\(2021\)694680_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf) (Acc. Oct. 31).
- European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies (2021b) *Update the Unfair Contract Terms Directive for Digital Services*, Study PE 676.006, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU\(2021\)676006_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf) (Acc. Oct. 31).
- European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies (2023) *Metaverse*, Study PE 751.222, [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU\(2023\)751222_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf) (Acc. Oct. 31).
- European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies (2020) *New Aspects and Challenges in Consumer Protection: Digital Services and Artificial Intelligence*, Study PE 648.790, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648790/IPOL_STU\(2020\)648790_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648790/IPOL_STU(2020)648790_EN.pdf) (Acc. Oct. 31).
- European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies (2021) *Online Advertising: The Impact of Targeted Advertising on Advertisers, Market Access and Consumer Choice*. Study PE 662.913.

BIBLIOGRAPHY

- [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU\(2021\)662913_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf) (Acc. Oct. 31).
- Eurostat Press Release. “What Did We Use the Internet for in 2022?.” December 15, 2022. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20221215-2> (Accessed February 23, 2023).
- Non-EU Policy Documents
- Autorité de la concurrence (2018) *Opinion No. 18-A-03 of March 2018 on Data Processing in the Online Advertising Sector* (Fr.) https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2019-10/avis18a03_en.pdf (Acc. Oct. 31).
- Autorité de protection des données Gegevensbeschermingsautoriteit Press Release. “IAB Europe Case: The Market Court Refers Preliminary Questions to the Court of Justice of the EU.” July 9, 2022 (Be.) <https://www.dataprotectionauthority.be/citizen/iab-europe-case-the-market-court-refers-preliminary-questions-to-the-court-of-justice-of-the-eu> (Accessed November 2, 2023).
- Autorité de protection des données Gegevensbeschermingsautoriteit (2022). “Klacht inzake Transparency & Consent Framework”. Februari, 2022, DOS-2019-01377 (Be.) <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022.pdf> (accessed November 2, 2023).
- Bundeskartellamt [BKartA] Case VI-Kart 1/19 (V), Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (Facebook), 26 August 2019, ECLI:DE:OLGD:2019:0826.VIKART1.19V.0A (Ger.)
- Bundeskartellamt Press Release. “CJEU Decision in Facebook Proceeding: Bundeskartellamt May Take Data Protection Rules into Consideration.” July 4, 2023. BUNDESKARTELLAMT (Ger.) https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/04_07_2023_EuGH.html. (Accessed April 7, 2023.)
- Comisión Nacional Del Mercado De Valores (2021) *Study On The Competition Conditions in The Online Advertising Sector in Spain* (Sp.) https://www.cnmc.es/sites/default/files/3696007_1.pdf (Acc. Oct. 31).
- Competition & Markets Authority (2020) *Online Platforms and Digital Advertising: Market Study – Final Report* (UK) <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/> (Acc. Oct. 31).
- Data Protection Commission (2021). “Fundamentals for a Child-Oriented Approach to Data Processing.” (Ir.) <https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing> (Accessed November 2, 2023).
- Datatilsynet (2021). “Administrative Fine - Grinder LLC.” Data Protection Authority (Nor.) <https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf> (Accessed November, 2023).
- Digital Competition Expert Panel (2019) “Unlocking Digital Competition: Report of the Digital Competition Expert Panel.” (UK) https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf (accessed November 2, 2023).
- European Court of Human Rights (2022) *Guide on Article 5 of the European Convention on Human Rights* (ECtHR) https://www.echr.coe.int/documents/d/echr/guide_art_5_eng (Acc. Oct. 31).

BIBLIOGRAPHY

- Federal Trade Commission (2013). *Com Disclosures: How to Make Effective Disclosures in Digital Advertising* (US) <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf> (Acc. Oct. 31)
- Federal Trade Commission Press Release. “FTC to Ban BetterHelp from Revealing Consumers’ Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising.” March 2, 2023. <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>.
- Forbrukerrådet (2018). *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*. The Consumer Council of Norway (Nor.) <https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf> (Acc. Oct. 31).
- Min. Economische Zaken (2009), *Strposchade – Rapport*, Den Haag: PRDF Advocaten 2009 (Neth.) Available at: <https://dendrou.eu/gallery/2009%20strooischade-onderzoeksrapport.pdf> (Acc Nov. 2, 2023).
- Organisation for Economic Co-operation and Development (2019) *An Introduction to Online Platforms and Their Role in the Digital Transformation* (OECD) <http://doi.org/10.1787/53e5f593-en> (Acc. Oct. 31).
- Stigler Committee (2019) *Digital Platforms – Final Report* (US) <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/policy-brief---digital-platforms---stigler-center.pdf> (Accessed October 31, 2023).

Academic Literature

- Acar, Gunes and Eubank, Christian and Englehardt, Steven and Juarez, Marc and Narayanan, Arvind and Diaz, Claudia (2014) “The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.” In *CCS '14: Proceedings of the 2014 ACM SIGSAC*. <https://doi.org/10.1145/2660267.2660347>.
- Aguirre, Elizabeth, and Mahr, Dominik and Grewal, Dhruv and Ruyter, Ko de and Wetzels, Martin (2015). “Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness.” *Journal of Retailing* 91 (1): 34–49. <https://doi.org/10.1016/j.jretai.2014.09.005>.
- Albæk, Svend (2013). “Consumer Welfare in EU Competition Policy.” In *Aims and Values in Competition Law*, by Caroline Heide-Jørgensen, Christian Bergqvist, Ulla B. Neergaard, and Sune Troels Poulsen (eds.). DJØF Publishing.
- AlHanai, Tuka, and Ghassemi, Mohammad (2017). “Predicting Latent Narrative Mood Using Audio and Physiologic Data.” *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence* 31 (1). <https://doi.org/10.1609/aaai.v31i1.10625>.
- Ali, Muhammad, and Sapiezynski, Piotr and Bogen, Miranda and Korolova, Aleksandra, and Mislove, Alan and Rieke, Aaron (2019). “Discrimination through Optimization: How Facebook’s Ad Delivery Can Lead to Skewed Outcomes.” *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–30. <https://doi.org/10.1145/3359301>.
- Alruwaily, Amaal, and Mangold, Chelsea and Greene, Tenay and Arshonsky, Josh and Cassidy, Omni and Pomeranz, Jennifer L. and Bragg, Marie (2020). “Child Social Media Influencers and Unhealthy Food Product Placement.” *Pediatrics* 146 (5): 20194057. <https://doi.org/10.1542/peds.2019-4057>.

BIBLIOGRAPHY

- Altman, Micah, Alexandra Wood, David R O'Brien, and Urs Gasser (2018). "Practical Approaches to Big Data Privacy over Time." *International Data Privacy Law* 8 (1): 29–51. <https://doi.org/10.1093/idpl/ix027>.
- An, Soontae, Gayle Kerr, and Hyun Seung Jin (2019). "Recognizing Native Ads as Advertising: Attitudinal and Behavioral Consequences." *Journal of Consumer Affairs* 53 (4): 1421–42. <https://doi.org/10.1111/joca.12235>.
- Ang, Ien (1991). *Desperately Seeking the Audience*. London: Routledge.
- Arvidsson, Adam (2003). "On the 'Pre-History of The Panoptic Sort': Mobility in Market Research." *Surveillance & Society* 1 (4). <https://doi.org/10.24908/ss.v1i4.3331>.
- Baldwin, Robert, and Cave, Martijn (2012). *Understanding Regulation: Theory Strategy, and Practice*. (2nd ed).
- Bartholomew, Abigail (2013). "Behaviorism's Impact on Advertising: Then and Now." Thesis. The College of Journalism and Mass Communications. Available at: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1042&context=journalismdiss>. Accessed November 2, 2023.
- Baumgartner, Susanne E, and Schuur, Winneke A van der, and Lemmens, Jeroen S. and Poel, Fam te (2018). "The Relationship Between Media Multitasking and Attention Problems in Adolescents: Results of Two Longitudinal Studies." *Human Communication Research* 44 (1): 3–30. <https://doi.org/10.1093/hcre.12111>.
- Bell, Daniel (2022). "Communitarianism." In *The Stanford Encyclopedia of Philosophy*, by Edward N. Zalta and Uri Nodelman (eds.), Fall 2022. Metaphysics Research Lab, Stanford University. <https://plato.stanford.edu/archives/fall2022/entries/communitarianism/> (Accessed November 2, 2023).
- Benedicte Fauvarque-Cosson (2011). "The Need for Codified Guiding Principles and Model Rules in European Contract Law." In *The Foundations of European Private Law*, Roger Brownsword, Hans-W Micklitz, Leone Niglia, and Stephen Weatherill (eds.). Hart Publishing. 2011. <https://hdl.handle.net/1814/20135>.
- Benkler, Yochai, and Farris, Robert and Roberts, Hal (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press. <https://doi.org/10.1093/oso/9780190923624.001.0001>.
- Berlin, Isaiah (1969). "Four Essays On Liberty." In *Two Concepts of Liberty*, 118–72. Oxford University Press.
- Bietti, Elettra (2022). "Structuring Digital Platform Markets: Antitrust and Utilities' Convergence" (November 11, 2022). University of Illinois Law Review, Vol. 2024 (4), Available at SSRN: <https://ssrn.com/abstract=4275143> or <http://dx.doi.org/10.2139/ssrn.4275143>.
- Bietti, Elettra (2023). "A Genealogy of Digital Platform Regulation." 7 *Georgetown Law Technology Review* 1.
- Binder, Alice, and Stubenvoll, Marlis and Hirsch, Melanie and Matthes, Jörg (2023). "Why Am I Getting This Ad? How the Degree of Targeting Disclosures and Political Fit Affect Persuasion Knowledge, Party Evaluation, and Online Privacy Behaviors." *Journal of Advertising* 51 (2). <https://doi.org/10.1080/00913367.2021.2015727>.
- Binns, Reuben, and Lyngs, Ulrik and Kleek, Max Van and Zhao, Jun and Libert, Timothy and Shadbolt, Nigel (2018). "Third Party Tracking in the Mobile Ecosystem." In *Proceedings of the 10th ACM Conference on Web Science*, 23–31. <https://doi.org/10.1145/3201064.3201089>.
- Boer, Maartje, and Stevens, Gonneke and Finkenauer, Catrin and Eijnden, Regina van den (2020). "Attention Deficit Hyperactivity Disorder-Symptoms, Social Media Use Intensity, and Social Media Use Problems in Adolescents: Investigating

BIBLIOGRAPHY

- Directionality.” *Child Development* 91 (4): e853–65. <https://doi.org/10.1111/cdev.13334>.
- Boerman, Sophie C., and Kruijkemeier, Sanne and Zuiderveen Borgesius, Frederik J. (2017). “Online Behavioral Advertising: A Literature Review and Research Agenda.” *Journal of Advertising* 46 (3): 363–76. <https://doi.org/10.1080/00913367.2017.1339368>.
- Boerman, Sophie C., and Reijmersdal, Eva A. van and Rozendaal, Esther and Dima, Alexandra L. (2018). “Development of the Persuasion Knowledge Scales of Sponsored Content (PKS-SC).” *International Journal of Advertising* 37 (5): 671–97. <https://doi.org/10.1080/02650487.2018.1470485>.
- Braun, Frederik (2012) “Origin Policy Enforcement in Modern Browsers.” Thesis. Ruhr Universitat Bochum. Available at: <https://frederik-braun.com/publications/thesis/Thesis-Origin Policy Enforcement in Modern Browsers.pdf> (Accessed November 2, 2023).
- Brenncke, Martin (2018). “The Legal Framework for Financial Advertising: Curbing Behavioural Exploitation.” *European Business Organization Law Review* 19 (4): 853–82. <https://doi.org/10.1007/s40804-018-0111-9>.
- Brin, Sergey and Page, Lawrence (1998). “The Anatomy of a Large Scale Hypertextual Web Search Engine.” *Computer Networks and ISDN Systems* 30: 107–17. <https://snap.stanford.edu/class/cs224w-readings/Brin98Anatomy.pdf>.
- Brooks, S. J., V. Savov, E. Allzén, C. Benedict, R. Fredriksson, and H. B. Schiöth (2012). “Exposure to Subliminal Arousing Stimuli Induces Robust Activation in the Amygdala, Hippocampus, Anterior Cingulate, Insular Cortex and Primary Visual Cortex: A Systematic Meta-Analysis of fMRI Studies.” *NeuroImage* 59 (3): 2962–73. <https://doi.org/10.1016/j.neuroimage.2011.09.077>.
- Burke, John J. A. (2000). “Contract as Commodity: A Nonfiction Approach.” *Seton Hall Legislative Journal* 24 (February): 285. Available at: <https://scholarship.shu.edu/shlj/vol24/iss2/4>.
- Burkeman, Oliver (2021). *Four Thousand Weeks: Time Management for Mortals*. Farrar, Straus and Giroux.
- Burri, Susanne (2015). “A Rights-Based Perspective on Permissible Harm.” Thesis. London School of Economics and Political Science. Available at: <http://etheses.lse.ac.uk/1060/> (Accessed November 2, 2023).
- Busch, Christoph, and Mak, Vanessa (2021). “Putting the Digital Services Act in Context.” *Journal of European Consumer and Market Law* 10 (3). <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\EuCML\EuCML2021025.pdf>.
- Calo, Ryan (2011). “The Boundaries of Privacy Harm.” *86 Indiana Law Journal* 1131 (2011) (3). <https://www.repository.law.indiana.edu/ilj/vol86/iss3/8>.
- Calo, Ryan (2014). “Digital Market Manipulation.” *82 George Washington Law Review* (995). <https://doi.org/10.2139/ssrn.2309703>.
- Cara, Corina (2019). “Dark Patterns In The Media: A Systematic Review.” *Network Intelligence Studies* VII (14): 105–13. https://seaopenresearch.eu/Journals/articles/NIS_14_3.pdf (Acc. Oct 31).
- Cave, Eric M. (2007). “What’s Wrong with Motive Manipulation?” *Ethical Theory and Moral Practice* 10 (2): 129–44. <https://doi.org/10.1007/s10677-006-9052-4>.
- Cave, Eric M. (2014). “Unsavoury Seduction and Manipulation,” In *Manipulation: Theory and Practice*, by Christian Coons and Michael Weber (eds.), 176-200.

BIBLIOGRAPHY

- Celis, L. Elisa, and Mehrotra, Anay and Vishnoi, Nisheeth K. (2019). "Toward Controlling Discrimination in Online Ad Auctions." arXiv (May, 2019). <https://doi.org/10.48550/arXiv.1901.10450>.
- Chang BA, Susie (1998). "Internet Segmentation: State-of-the-Art Marketing Applications: Journal of Segmentation in Marketing: Vol 2, No 1." *Journal of Segmentation in Marketing* 2 (1): 19–34. https://doi.org/10.1300/J142v02n01_03.
- Chen, Jiahong (2021). *Regulating Online Behavioural Advertising Through Data Protection Law*. Regulating Online Behavioural Advertising Through Data Protection Law. Edward Elgar Publishing. <https://www.elgaronline.com/display/9781839108297.00015.xml>.
- Cialdini, Robert B. (2007). *Influence: The Psychology of Persuasion*. Revised edition.; First Collins business essentials edition. Collins Business Essentials. New York: Collins Business.
- Citron, Daniel Keats, and Solove, Daniel J. (2022). "Privacy Harms." *Boston University Law Review* 102 (793). Available at: <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>.
- Cohen, Julie E. (2017). "Law for the Platform Economy." *U.C. Davis Law Review* 51 (133). https://lawreview.law.ucdavis.edu/issues/51/1/symposium/51-1_Cohen.pdf.
- Cohen, Julie E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York: Oxford University Press. <https://doi.org/10.1093/oso/9780190246693.001.0001>.
- Cohen, Julie E. (2023). "Infrastructuring the Digital Public Sphere." 25 Yale J.L. & Tech. Special Issue 1, 1-40. https://yjolt.org/sites/default/files/cohen_julie_-_infrastructuring_the_digital_public_sphere.01.pdf.
- Coons, Christian and Weber, Michael (eds) (2014b) *Manipulation: Theory and Practice*. New York: Oxford University Press.
- Coons, Christian, and Weber, Michael (2014a). "Introduction: Manipulation: Investigating the Core Concept and Its Moral Status." In *Manipulation: Theory and Practice*, by Christian Coons and Michael Weber (eds.).
- Corrêa, Ana Maria (2022). "Regulating Targeted Advertising: Addressing Discrimination with Transparency, Fairness, and Auditing Tests Remedies." *Computer Law & Security Review* 46 (September): 105732. <https://doi.org/10.1016/j.clsr.2022.105732>.
- Crawford, Kate (2021). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.
- Creemers, Rogier (2018). "China's Social Credit System: An Evolving Practice of Control." Available at SSRN: <https://ssrn.com/abstract=3175792> or <http://dx.doi.org/10.2139/ssrn.3175792>.
- Croes, Marnix (2006). "The Holocaust in the Netherlands and the Rate of Jewish Survival." *Holocaust and Genocide Studies* 20 (3): 474–99. <https://doi.org/10.1093/hgs/dcl022>.
- Cseres, Kati J. (2024). "EU Competition Law and Democracy in the Shadow of Rule of Law Backsliding", THE EVOLVING GOVERNANCE OF EU COMPETITION LAW IN A TIME OF DISRUPTIONS: A CONSTITUTIONAL PERSPECTIVE (C. Colombo & M. Eliantonio, K. Wright, eds.)
- Curti, Merle (1967). "The Changing Concept of 'Human Nature' in the Literature of American Advertising." *The Business History Review* 41 (4): 335–57. <https://doi.org/10.2307/3112645>.
- Custers, Bart (2004). "The Power of Knowledge Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology." Tilburg: Wolf Legal Publishers. Available at SSRN: <https://papers.ssrn.com/abstract=3186639>.

BIBLIOGRAPHY

- Custers, Bart, and Fosch-Villaronga, Eduard and Hof, Simone van der and Schermer, Bart and Sears, Alan M. and Tamò-Larrieux, Aurelia (2022). “The Role of Consent in an Algorithmic Society - Its Evolution, Scope, Failings and Re-Conceptualization.” In *Research Handbook on EU Data Protection Law* by Eleni Kosta and Ronald Leenes (eds.), 455–73. Edward Elgar Publishing.
- Custers, Bart, and Malgieri, Gianclaudio (2022). “Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data.” *Computer Law & Security Review* 45 (July): 105683. <https://doi.org/10.1016/j.clsr.2022.105683>.
- Datta, Amit, and Datta, Makagon and Anupam Jael and Mulligan, Deirdre K. and Tschantz, Michael Carl (2018). “Discrimination in Online Advertising: A Multidisciplinary Inquiry.” In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 20–34. PMLR. <https://proceedings.mlr.press/v81/datta18a.html>.
- Davola, Antonio and Malgieri, Gianclaudio (2022). “Data, Power and Competition Law: The (Im)Possible Mission of the DMA?” *Research in Law and Economics*, (forthcoming, 2023). Available at SSRN: <https://ssrn.com/abstract=4242574> or <http://dx.doi.org/10.2139/ssrn.4242574>.
- De Gregorio, Giovanni (2022). *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge Studies in European Law and Policy. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781009071215>.
- Dehling, Tobias, and Zhang, Yuchen and Sunyaev, Ali (2019). “Consumer Perceptions of Online Behavioral Advertising.” In *2019 IEEE 21st Conference on Business Informatics (CBI)*, Moscow, Russia, 2019, pp. 345-354. <https://ieeexplore.ieee.org/document/8808011>.
- Dupr, Catherine (2015). *The Age of Dignity: Human Rights and Constitutionalism in Europe*. 1st ed. London: Hart Publication Ltd.
- Economides, Nicholas and Lianos, Ioannis (2021). “Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective,” *Journal of Competition Law & Economics* 17 (4): 765–847. <https://doi.org/10.1093/joclec/nhab007>.
- Economides, Nicholas, and Lianos, Ioannis (2020). “Privacy and Antitrust in Digital Platforms.” NET Institute Working Paper No. #21-01, NYU Stern School of Business (forthcoming). See: <https://ssrn.com/abstract=3755327> or <https://doi.org/10.2139/ssrn.3755327>.
- Elroy, Boers, and Afzali, Mohammad H. and Conrod, Patricia (2020). “A Longitudinal Study on the Relationship between Screen Time and Adolescent Alcohol Use: The Mediating Role of Social Norms.” *Preventive Medicine* 132 (March): 105992. <https://doi.org/10.1016/j.ypmed.2020.105992>.
- Epictetus (2014). *Discourses, Fragments, Handbook*. Oxford World’s Classics.
- Eubanks, Virginia (2019). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish*. St. Martin's Press, Inc.
- Eyal, Nir (2014). *Hooked: How to Build Habit-Forming Products*. Portfolio Penguin, 2014.
- Ezrachi, Ariel and Stucke, Maurice E. (2016). “The Rise of Behavioural Discrimination.” *European Competition Law Review* 37 (August): 484. <https://doi.org/10.2139/ssrn.2830206>.
- Faddoul, Marc and Kapuria, Rohan and Lin, Lily (2019). “Sniper Ad Targeting.” *MIMS Final Project*.
- Fineman, Martha (2010). “The Vulnerable Subject and the Responsive State.” *Emory Law Journal* 60 (2): 251.
- Floridi, Luciano (2016). “On Human Dignity and a Foundation for the Right to Privacy.” *Philosophy & Technology* 29: 307-312 <https://doi.org/10.2139/ssrn.3839298>.

BIBLIOGRAPHY

- Floridi, Luciano (2021). “The European Legislation on AI: A Brief Analysis of Its Philosophical Approach.” *Philosophy & Technology* 34 (2): 215–22. <https://doi.org/10.1007/s13347-021-00460-9>.
- Florio, Massimo and Pancotti, Chiara (2022). *Applied Welfare Economics: Cost-Benefit Analysis of Projects and Policies*. 2nd ed. London: Routledge. <https://doi.org/10.4324/9781003191377>.
- Friestad, Marian, and Wright, Peter (1994). “The Persuasion Knowledge Model: How People Cope with Persuasion Attempts.” *Journal of Consumer Research* 21: 1–31. <https://doi.org/10.1086/209380>.
- Galli, Federico (2022). “Digital Vulnerability.” In *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, edited by Federico Galli, 181–207. Law, Governance and Technology Series. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-13603-0_7.
- Galli, Federico (2022a). *Algorithmic Marketing and EU Law on Unfair Commercial Practices*. Vol. 50. Law, Governance and Technology Series. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-031-13603-0>.
- Gardiner, Caterina (2022). *Unfair Contract Terms in the Digital Age*. Edward Elgar Publishing.
- Geradin, Damien, and Katsifis, Dimitrios (2019). “An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age.” *European Competition Journal* 15 (1): 55–96. <https://doi.org/10.1080/17441056.2019.1574440>.
- Goanta, Catalina, and Ranchordás, Sofia (eds.) (2020). *The Regulation of Social Media Influencers*. Elgar Law, Technology and Society Series. Edward Elgar Publishing. <https://doi.org/10.4337/9781788978286>.
- Goldenfein, Jake, and McGuigan, Lee. (2023). “Managed Sovereigns: How Inconsistent Accounts of the Human Rationalize Platform Advertising.” *Journal of Law and Political Economy* 3 (3). <https://doi.org/10.5070/LP63361141>.
- González Fuster, Gloria (2014). “EU Fundamental Rights and Personal Data Protection.” In *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, by Gloria González Fuster (ed.), 163–212. Law, Governance and Technology Series. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-05023-2_6.
- Goodin, Robert E. (1986). *Protecting the Vulnerable: A Re-Analysis of Our Social Responsibilities*. Chicago, IL: University of Chicago Press.
- Graef, Inge (2021). “Consumer Sovereignty and Competition Law: From Personalization to Diversity.” *Common Market Law Review* 58 (2): 471–504.
- Griffin, James (2008). “Autonomy.” In *On Human Rights*, edited by James Griffin, 0. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199238781.003.0009>.
- Groot, Judith Irene Maria de. (2022). “The Personalization Paradox in Facebook Advertising: The Mediating Effect of Relevance on the Personalization–Brand Attitude Relationship and the Moderating Effect of Intrusiveness.” *Journal of Interactive Advertising* 22 (1): 57–74. <https://doi.org/10.1080/15252019.2022.2032492>.
- Hacker, Philipp (2021). “Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law.” *European Law Journal* 1–34 <https://doi.org/10.1111/eulj.12389>.
- Hannak, Aniko and Soeller, Gary and Lazer, David and Mislove, Alan and Wilson, Christo (2014). “Measuring Price Discrimination and Steering on E-Commerce Web Sites.” In *Proceedings of the 2014 Conference on Internet Measurement Conference*, 305–18. Vancouver BC Canada: ACM. <https://doi.org/10.1145/2663716.2663744>.

BIBLIOGRAPHY

- Hanson, Jon D., and Kysar, Douglas A (1999). "Taking Behavioralism Seriously: The Problem of Market Manipulation." *NYU Law Review* 74 (3): 630–749.
- Hanson, Jon D., and Kysar, Douglas A. (2000). "Taking Behavioralism Seriously: A Response to Market Manipulation." *6 Roger Williams U. L. Rev.* 259. Available at: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:3175148>.
- Hartmann, Patrick, and Marcos, Aitor and Castro, Juana and Apaolaza, Vanessa (2023). "Perspectives: Advertising and Climate Change – Part of the Problem or Part of the Solution?" *International Journal of Advertising* 42 (2): 430–57. <https://doi.org/10.1080/02650487.2022.2140963>.
- Hayek, Friedrich A (2013). *The Market and Other Orders*. Edited by Bruce Caldwell.
- He, Qinghua, and Turel, Ofir and Bechara, Antoine (2017). "Brain Anatomy Alterations Associated with Social Networking Site (SNS) Addiction." *Scientific Reports* 7 (1): 45064. <https://doi.org/10.1038/srep45064>.
- Heimann, Jim (1999). *The Golden Age of Advertising: The 50s*. TASCHEN's 25th anniversary special edition. Barnes & Noble.
- Helberger, Natali, and Lynskey, Orla, and Micklitz, Hans-Wolfgang and Rott, Peter and Sax, Marijn and Strycharz, Joanna (2021). "EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets, A Joint Report from Research Conducted under the EUCP2.0 Project" <https://dare.uva.nl/search?identifier=81f5aca7-6b01-4ade-90fa-e02d3024bc3a> (accessed November 2, 2023).
- Helberger, Natali, and Sax, Marijn and Strycharz, Joanna and Micklitz Hans-Wolfgang (2022). "Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability." *Journal of Consumer Policy* 45 (2): 175–200. <https://doi.org/10.1007/s10603-021-09500-5>.
- Helberger, Natali, and Zuiderveen Borgesius, Frederik and Reyna, Agustin (2017). "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law." *Common Market Law Review* 54 (5).
- Herring, Jonathan (2019). *Law and the Relational Self*. 1st ed. Cambridge University Press. <https://doi.org/10.1017/9781108348171>.
- Hildebrandt, Mireille (2008). "Defining Profiling: A New Type of Knowledge?" In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 17–45. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-6914-7_2.
- Hirsh, Jacob B. and Kang, Sonia K. and Bodenhausen, Galen V. (2012). "Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits." *Psychological Science* 23 (6): 578–81.
- Howard, John A. and Hulbert, James (1973). "Advertising and The Public Interest: A Staff Report to the Federal Trade Commission." ED 074777.
- Hutton, John S. and Dudley, Jonathan and Horowitz-Kraus, Tzipi and DeWitt, Tom and Holland, Scott K. (2020). "Associations Between Screen-Based Media Use and Brain White Matter Integrity in Preschool-Aged Children." *JAMA Pediatrics* 174 (1): e193869. <https://doi.org/10.1001/jamapediatrics.2019.3869>.
- Huxley, Aldous (1932). *Brave New World*. Vintage.
- Jadil, Yassine, and Rana, Nripendra P. and Dwivedi, Yogesh K. (2022). "Understanding the Drivers of Online Trust and Intention to Buy on a Website: An Emerging Market Perspective." *International Journal of Information Management Data Insights* 2 (1): 100065. <https://doi.org/10.1016/j.ijime.2022.100065>.
- Jagielska, Monika, and Jagielski, Mariusz (2012). "Are Consumer Rights Human Rights?" In *European Consumer Protection: Theory and Practice*, James Devenney and Mel

BIBLIOGRAPHY

- Kenny (eds.), 336–53. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781139003452.021>.
- Jones, Alison and Sufrin, Brenda (2011). *EU Competition Law: Text, Cases, and Materials*. Fourth. Oxford University Press.
- Jongepier, Fleur, and Klenk, Michael (2022). *The Philosophy of Online Manipulation*. 1st ed. New York: Routledge. <https://doi.org/10.4324/9781003205425>.
- Kahneman, Daniel (2011). *Thinking Fast and Slow*. Farrar, Straus and Giroux.
- Kant, Immanuel (2019). *Groundwork for the Metaphysics of Morals*. Oxford University Press.
- Karaj, Arjaldo, and Macbeth, Sam and Berson, Rémi and Pujol, Josep M. (2019). “WhoTracks .Me: Shedding Light on the Opaque World of Online Tracking.” arXiv (April 2019). <https://doi.org/10.48550/arXiv.1804.08959>.
- Kaushik, Basu, and Luis F. López-Calva (2011). “Functionings and Capabilities.” In *Handbook of Social Choice and Welfare*, by Kenneth J. Arrow, Amartya Sen, and Kotaro Suzumura (eds.), 2:153–87. Handbook of Social Choice and Welfare. Elsevier. [https://doi.org/10.1016/S0169-7218\(10\)00016-X](https://doi.org/10.1016/S0169-7218(10)00016-X).
- Kennedy, Duncan (2011). “A Transnational Genealogy of Proportionality in Private Law.” In *The Foundations of European Private Law*, by Roger Brownsword, Hans-W Micklitz, Leone Niglia, and Stephen Weatherill (eds.)
- Keymolen, Esther (2018). “Trust In the Networked Era: When Phones Become Hotel Keys.” *Techne: Research in Philosophy and Technology* 22 (1): 51-75. <https://doi.org/10.5840/techne201792271>.
- Kilovaty, Ido (2019). “Legally Cognizable Manipulation.” *Berkeley Technology Law Journal* 34: 449–501. <https://doi.org/10.2139/ssrn.3224952>.
- Kilovaty, Ido (2021). “Psychological Data Breach Harms,” *North Carolina Journal of Law & Technology* 23 (1): 1. Available at: <https://scholarship.law.unc.edu/ncjolt/vol23/iss1/2>.
- Kim, Tami, and Barasz, Kate and John, Leslie K. (2019). “Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness.” by Eileen Fischer and Andrea Morales (eds.). *Journal of Consumer Research* 45 (5): 906–32. <https://doi.org/10.1093/jcr/ucy039>.
- Klenk, Michael (2022). “(Online) Manipulation: Sometimes Hidden, Always Careless.” *Review of Social Economy* 80 (1): 85–105. <https://doi.org/10.1080/00346764.2021.1894350>.
- Koolen, Christof (2023). “Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data.” *European Review of Private Law* 31 (2/3). <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\ERPL\ERPL2023018.pdf>.
- Kosinski, Michal, and Stillwell, David and Graepel, Thore (2013). “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior.” *Proceedings of the National Academy of Sciences* 110 (15): 5802–5. <https://doi.org/10.1073/pnas.1218772110>.
- Lanzing, Marolijn (2019). “The Transparent Self: A Normative Investigation of Changing Selves And Relationships In The Age Of Quantified Self.” Thesis. Eindhoven University of Technology. Available at: https://pure.tue.nl/ws/portalfiles/portal/140533915/20191211_Lanzing.pdf.
- Laux, Johann (2021b) “Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA.” *Computer Law & Security Review* 43 (November): 105613. <https://doi.org/10.1016/j.clsr.2021.105613>.

BIBLIOGRAPHY

- Laux, Johann, and Wachter, Sandra and Mittelstadt, Brent (2021a). “Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice.” *Common Market Law Review* 58 (3): 719-750. <https://doi.org.ezproxy.leidenuniv.nl/10.54648/cola2021048>.
- Lee, Jenny (2020). “The Google-DoubleClick Merger: Lessons From the Federal Trade Commission’s Limitations on Protecting Privacy.” *Communication Law and Policy* 25 (1): 77–103. <https://doi.org/10.1080/10811680.2020.1690330>.
- Lee, Jin-Myong, and Rha, Jong-Youn (2016). “Personalization–Privacy Paradox and Consumer Conflict with the Use of Location-Based Mobile Commerce.” *Computers in Human Behavior* 63 (October): 453–62. <https://doi.org/10.1016/j.chb.2016.05.056>.
- Leiser, Mark R. (2022). “Dark Patterns: The Case for Regulatory Pluralism Between the European Unions Consumer and Data Protection Regimes.” In *Research Handbook on EU Data Protection Law*, by Eleni Kosta and Ronald Leenes (eds.) 240–69. Edward Elgar Publishing.
- Lemley, Mark A. (2022) “The Benefit of the Bargain” (August 8, 2022). Stanford Law and Economics Olin Working Paper 575. Available at: SSRN <https://ssrn.com/abstract=4184946> or <https://dx.doi.org/10.2139/ssrn.4184946>.
- Lemley, Mark A. 1995. “Intellectual Property and Shrinkwrap Licenses.” *Southern California Law Review* 68 (1239). Available at SSRN: <https://ssrn.com/abstract=2126845> or <http://dx.doi.org/10.2139/ssrn.2126845>.
- LiKamWa, Robert, and Liu, Yunxin and Lane, Nicholas D. and Zhong, Lin (2013). “MoodScope: Building a Mood Sensor from Smartphone Usage Patterns.” In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, 389–402. MobiSys ’13. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/2462456.2464449>.
- Lingel, Jessa (2020). *An Internet for the People: The Politics and Promise of Craigslist*. Princeton Studies in Culture and Technology Series. Princeton University Press. <https://doi.org/10.2307/j.ctvp2n5q4>.
- Loos, Marco and Helberger, Natali and Guibault, Lucie and Mak, Chantal (2011). “The Regulation of Digital Content Contracts in the Optional Instrument of Contract Law.” *European Review of Private Law* 6: 729–58. <https://hdl.handle.net/11245/1.353862>.
- Luna, Florencia (2019). “Identifying and Evaluating Layers of Vulnerability – A Way Forward.” *Developing World Bioethics* 19 (2): 86–95. <https://doi.org/10.1111/dewb.12206>.
- Machiavelli, Niccolò (2006). *The Prince*. Translated by W. K. (William Kenaz) Marriott. Project Gutenberg (eBook).
- Mackenzie, Catriona, Rogers, Wendy and Dodds, Sandy (eds.) (2014). *Vulnerability: New Essays in Ethics and Feminist Philosophy*. Studies in Feminist Philosophy. New York: Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199316649.001.0001>.
- Mak, Vanessa (2016). “The Consumer in European Regulatory Private Law. A Functional Perspective on Responsibility, Protection and Empowerment.” In *The Image(s) of the Consumer in EU Law: Legislation, Free Movement and Competition Law*, by Dorota Leczykiewicz and Stephen Weatherill (eds.), 381–400. Oxford: Hart Publishing.
- Mak, Vanessa (2022). “A Primavera for European Consumer Law: Re-Birth of the Consumer Image in the Light of Digitalisation and Sustainability.” *Journal of European Consumer and Market Law* 11 (3): 77–80.

BIBLIOGRAPHY

- Malgieri, Gianclaudio (2020). "The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation." In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 154–66. FAT* '20. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372868>.
- Malgieri, Gianclaudio, and Custers Bart (2017). "Pricing Privacy – The Right to Know the Value of Your Personal Data." *Computer Law & Security Review* 34 (2): 289–303. <https://doi.org/doi:10.1016/j.clsr.2017.08.006>.
- Malgieri, Gianclaudio, and Davola, Antonio. 2022. "Data-Powerful." Available at SSRN: <https://ssrn.com/abstract=4027370> or <http://dx.doi.org/10.2139/ssrn.4027370>.
- Malgieri, Gianclaudio, and Niklas, Jędrzej (2020). "Vulnerable Data Subjects." *Computer Law and Security Review* 37 (July). <https://doi.org/10.1016/j.clsr.2020.105415>.
- Marcuse, Herbert (1965). "Industrialization and Capitalism." *New Left Review*, no. 1/30 (April): 3–17.
- Marotta, Veronica, and Wu, Yue and Zhang, Kaifu and Acquisti, Alessandro (2022). "The Welfare Impact of Targeted Advertising Technologies." *Information Systems Research* 33 (1): 131–51. <https://doi.org/10.1287/isre.2021.1024>.
- Mathur, Arunesh, and Mayer, Jonathan and Kshirsagar, Mihir (2021). "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*, 1–18. <https://doi.org/10.1145/3411764.3445610>.
- Matz, Sandra C, and Appel, Ruth E. and Kosinski, Michal (2020). "Privacy in the Age of Psychological Targeting." *Current Opinion in Psychology*, Privacy and Disclosure, Online and in Social Interactions, 31 (February): 116–21. <https://doi.org/10.1016/j.copsyc.2019.08.010>.
- Maurits, Kaptein (2015). *Persuasion Profiling: How the Internet Knows What Makes You Tick*. Business Contact.
- McCann, Michael A. (2014). "Dietary Supplement Labeling: Cognitive Biases, Market Manipulation & Consumer Choice." *American Journal of Law & Medicine* 31 (2–3): 215–68. <https://doi.org/10.1177/009885880503100204>.
- McCrudden, Christopher (2008). "Human Dignity and Judicial Interpretation of Human Rights." *European Journal of International Law* 19 (4): 655–724. <https://doi.org/10.1093/ejil/chn043>.
- Mill, John Stuart (2011). *Essays on Some Unsettled Questions of Political Economy*. Luton: Andrews UK (eBook ed.).
- Mill, John Stuart (2011). *On Liberty*. Cambridge University Press (1st ed. 1859). <https://doi-org.ezproxy.leidenuniv.nl/10.1017/CBO9781139149785>.
- Millns, Susan (1996). "Dwarf-Throwing and Human Dignity: A French Perspective." *Journal of Social Welfare and Family Law* 18 (3): 375–91. <https://doi.org/10.1080/09649069608410182>.
- Moon, Youngme (2002). "Personalization and Personality: Some Effects of Customizing Message Style Based on Consumer Personality." *Journal of Consumer Psychology* 12 (4): 313–25. [https://doi.org/10.1016/S1057-7408\(16\)30083-3](https://doi.org/10.1016/S1057-7408(16)30083-3).
- Moore, Robert, and Moore, Melissa and Shanahan, Kevin and Horky, Alisha and Britney Mack (2015). "Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation." *The Marketing Management Journal* 25 (1): 42–53.
- Morel, Victor, and Santos, Cristiana and Fredholm, Viktor and Thunberg, Adam (2023). "Legitimate Interest Is the New Consent -- Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls." arXiv (September 2023) <https://arxiv.org/abs/2309.11625v3>.

BIBLIOGRAPHY

- Morey, Timothy, and Forbath, Theodore, and Schoop, Allison (2015). "Customer Data: Designing for Transparency and Trust." *Harvard Business Review*, May 1, 2015. <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.
- Moriarty, Jeffrey (2021). "Why Online Personalized Pricing Is Unfair." *Ethics and Information Technology* 23 (3): 495–503. <https://doi.org/10.1007/s10676-021-09592-0>.
- Musgrave, Richard A. (2017). "Merit Goods." In *The New Palgrave Dictionary of Economics*, 1–5. London: Palgrave Macmillan UK. https://doi.org/10.1057/978-1-349-95121-5_1139-2.
- Neal, Mary (2012). "Not Gods but Animals: Human Dignity and Vulnerable Subjecthood." *Liverpool Law Review* 23 (3): 177–200. <https://doi.org/10.1007/s10991-012-9124-6>.
- Nielsen, Janne (2021). "Using Mixed Methods to Study the Historical Use of Web Beacons in Web Tracking." *International Journal of Digital Humanities* 2 (November): 1–24. <https://doi.org/10.1007/s42803-021-00033-4>.
- Nikiforakis, Nick, and Kapravelos, Alexandros and Joosen, Wouter and Kruegel, Christopher and Piessens, Frank and Vigna, Giovanni (2013). "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting." In *2013 IEEE Symposium on Security and Privacy*, 541–55. IEEE Computer Society. <https://doi.org/10.1109/SP.2013.43>.
- Noggle, Robert (1996). "Manipulative Actions: A Conceptual and Moral Analysis." *American Philosophical Quarterly* 33 (1): 43–55. <https://www.jstor.org/stable/20009846>.
- Noggle, Robert (2018) "Manipulation, Salience, and Nudges," *Bioethics* 32 (3): 164–70. <https://doi.org/10.1111/bioe.12421>.
- Noggle, Robert (2020), "Pressure, Trickery, and a Unified Account of Manipulation," *American Philosophical Quarterly* 3 (57): 241–52.
- Noggle, Robert (2022). "The Ethics of Manipulation," In *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.). <https://plato.stanford.edu/archives/sum2022/entries/ethics-manipulation/> (Acc. Oct. 31).
- Nouwens, Midas, and Liccardi, Ilaria and Veale, Michael and Karger, David and Kagal, Lalana (2020). "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3313831.3376321>.
- Nussbaum, Martha C. (2007). *Frontiers of Justice: Disability, Nationality, Species Membership*. The Tanner Lectures on Human Values. Cambridge, MA: Belknap Press. <https://doi-org.ezproxy.leidenuniv.nl/10.2307/j.ctv1c7zftw>.
- Nussbaum, Martha C. (2011), *Creating Capabilities: The Human Development Approach*. Harvard University Press. <https://doi-org.ezproxy.leidenuniv.nl/10.2307/j.ctt2jbt31>.
- Nussbaum, Martha C. 1997. "Capabilities and Human Rights." *Fordham Law Review* 66 (2): 273. <https://ir.lawnet.fordham.edu/flr/vol66/iss2/2>.
- Nys, Thomas RV, and Engelen, Bart (2017). "Judging Nudging: Answering the Manipulation Objection." *Political Studies* 65 (1): 199–214. <https://doi.org/10.1177/0032321716629487>.
- O’Neil, Cathy (2017). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Penguin Books.
- Odlyzko, Andrew (2003). "Privacy, Economics, and Price Discrimination on the Internet." *ICEC2003: Fifth International Conference on Electronic Commerce*, N. Sadeh, (ed.), ACM, 2003, 355-366, Available at SSRN: <https://ssrn.com/abstract=429762> or <http://dx.doi.org/10.2139/ssrn.429762>.

BIBLIOGRAPHY

- Odlyzko, Andrew (2009). "Network Neutrality, Search Neutrality, and the Never-Ending Conflict between Efficiency and Fairness in Markets." *Review of Network Economics* 8 (1), 40-60 <https://doi.org/10.2202/1446-9022.1169>.
- Pachilakis, Michalis, and Papadopoulos, Panagiotis and Markatos, Evangelos P. and Kourtellis, Nicolas (2019). "No More Chasing Waterfalls: A Measurement Study of the Header Bidding Ad-Ecosystem." arXiv. <https://doi.org/10.48550/arXiv.1907.12649>.
- Packard, Vance (1957). *The Hidden Persuaders*. New York: David McKay.
- Pariser, Eli (2012). *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. Penguin Books. London.
- Park, Gregory, H. and Schwartz, Andrew and Eichstaedt, Johannes C. and Kern, Margaret L. and Kosinski, Michal and Stillwell, David J. and Ungar, Lyle H. and Seligman, Martin E. P. (2015). "Automatic Personality Assessment Through Social Media Language." *Journal of Personality and Social Psychology* 108: 934–52. <https://doi.org/10.1037/pspp0000020>.
- Pärssinen, Matti, and Kotila, Mikko, and Cuevas, Rubén and Phansalkar, Amit and Manner, Jukka M.J. (2018). "Environmental Impact Assessment of Online Advertising." *Environmental Impact Assessment Review* 73 (November): 177–200. <https://doi.org/10.1016/j.eiar.2018.08.004>.
- Pettit, Philip (2002). *Republicanism: A Theory of Freedom and Government*. Oxford Political Theory. Oxford: Clarendon Press.
- Pitofsky, Robert (1977). "Beyond Nader: Consumer Protection and the Regulation of Advertising." *Harvard Law Review* 90 (4): 661–701. <https://doi.org/10.2307/1340281>.
- Plantin, Jean-Christophe, Carl Lagoze, Paul N Edwards, and Christian Sandvig (2018). "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20 (1): 293–310. <https://doi.org/10.1177/1461444816661553>.
- Plato (2008). *Republic*. Oxford World's Classics.
- Preston, Ivan L. (1997). "Regulatory Positions toward Advertising Puffery of the Uniform Commercial Code and the Federal Trade Commission." *Journal of Public Policy & Marketing* 16 (2): 336–44. <https://www.jstor.org/stable/30000457>.
- Prosser, Tony (2006). "Regulation and Social Solidarity." *Journal of Law and Society* 33 (3): 364–87. <https://www.jstor.org/stable/3838855>.
- Purohit, Aditya Kumar, and Barclay, Louis and Holzer, Adrian (2020). "Designing for Digital Detox: Making Social Media Less Addictive with Digital Nudges." In . <https://dl.acm.org/doi/abs/10.1145/3334480.3382810>.
- Rajanala, Susruthi, and Maymone, Mayra B. C. and Vashi, Neelam A. (2018). "Selfies—Living in the Era of Filtered Photographs." *JAMA Facial Plastic Surgery* 20 (6): 443–44. <https://doi.org/10.1001/jamafacial.2018.0486>.
- Rathje, Steve and Van Bavel, Jay J., and van der Linden, Sander (2020) "Out-Group Animosity Drives Engagement on Social Media." *PNAS* 118(26): e2024292118 <https://doi.org/10.1073/pnas.2024292118>.
- Rawls, John (1971). *A Theory of Justice: Original Edition*. Harvard University Press. <https://doi.org/10.2307/j.ctvjf9z6v>.
- Richards, Neil M. (2013). "The Dangers of Surveillance." *Harvard Law Review* 126 (7): 1934–65. <https://www.jstor.org/stable/23415062>.
- Riddle, Elizabeth, and MacKay, Jill R. D. (2020). "Social Media Contexts Moderate Perceptions of Animals." *Animals: An Open Access Journal from MDPI* 10 (5): 845. <https://doi.org/10.3390/ani10050845>.
- Riley, Stephen (2013). "The Function of Dignity." *Amsterdam Law Forum* 5 (2) 90-106. Available at: <https://ssrn.com/abstract=2293363>.

BIBLIOGRAPHY

- Rimer, Barbara K., and Kreuter, Matthew W. (2006). "Advancing Tailored Health Communication: A Persuasion and Message Effects Perspective." *Journal of Communication* 56 (suppl_1): S184–201. <https://doi.org/10.1111/j.1460-2466.2006.00289.x>.
- Robeyns, Ingrid, and Byskov, Morten Fibieger (2023). "The Capability Approach." In *The Stanford Encyclopedia of Philosophy*, by Edward N. Zalta and Uri Nodelman (eds), Stanford University. <https://plato.stanford.edu/archives/sum2023/entries/capability-approach/>.
- Rodgers, Shelly, Hugh Cannon, and Jensen Moore (2007). "Segmenting Internet Markets." In *Internet Advertising: Theory and Research*, David W. Schumann and Esther Thorson (eds.), Mahwah, NJ: Lawrence Erlbaum Associates, 149–83.
- Roessler, Beate (2005). *The Value of Privacy*. Polity Press.
- Rogers, Wendy (2013). "Vulnerability and Bioethics." In *Vulnerability: New Essays in Ethics and Feminist Philosophy*, by Catriona Mackenzie, Wendy Rogers, and Susan Dodds (eds.), 60-87. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199316649.003.0003>.
- Rose, Blaire (2021). "The Commodification of Personal Data and The Road to Consumer Autonomy through the CCPA" 15 (521). <https://brooklynworks.brooklaw.edu/bjcfcl/vol15/iss2/8>.
- Rudinow, Joel (1978). "Manipulation." *Ethics* 88 (4): 338–47. <https://doi.org/10.1086/292086>.
- Salpeter, Laura R. and Swirsky, Jennifer I. (2012). "Historical and Legal Implications of Subliminal Messaging in the Multimedia: Unconscious Subjects." *Nova Law Review* 36 (3): 497–520.
- Santos, Cristiana, and Rossi, Arianna and Chamorro, Lorena Sanchez Bongard-Blanchy, Kerstin and Abu-Salma, Ruba (2021). "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*, 187–94. WPES '21. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3463676.3485611>.
- Sax, Marijn (2021). *Between Empowerment and Manipulation: The Ethics and Regulation of for-Profit Health Apps*. Information Law Series, 47. Alphen aan den Rijn, The Netherlands: Kluwer Law International B. V.
- Schermer, Bart W., Custers, Bart and van der Hof, Simone (2014). "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection." *Ethics and Information Technology* 16 (2): 171–82. <https://doi.org/10.1007/s10676-014-9343-8>.
- Schull, Natasha Dow (2014). *Addiction by Design*. Princeton University Press.
- Sears, Alan M (2021) "The Limits of Online Price Discrimination in Europe." *Science and Technology Law Review* 21 (1): 1–42. <https://doi.org/10.7916/stlr.v21i1.5761>.
- Seaton, A.V. (1986). "Cope's and the Promotion of Tobacco in Victorian England." *European Journal of Marketing* 20 (9): 5–26. <https://doi.org/10.1108/EUM0000000004664>.
- Segalin, Crisitina, and Perina, Alessandro and Cristani, Marco and Vinciarelli, Alessandro (2017). "The Pictures We Like Are Our Image: Continuous Mapping of Favorite Pictures into Self-Assessed and Attributed Personality Traits." *IEEE Transactions on Affective Computing* 8 (2): 268–85. <https://doi.org/10.1109/TAFFC.2016.2516994>.
- Simon, Herbert A. (1971). "Designing Organizations for an Information-Rich World." In *Computers, Communications, and the Public Interest*. The John Hopkins Press.

BIBLIOGRAPHY

- Sipior, Janice, and Ward, Burke and Mendoza, Rubén (2011). “Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons.” *Journal of Internet Commerce* 10 (March): 1–16. <https://doi.org/10.1080/15332861.2011.558454>.
- Smith, Adam (2000). *The Wealth of Nations*. Robert B. Reich (ed.). Westminster, US: Random House Publishing Group.
- Sobieszek, Robert A. (1988). *The Art of Persuasion: A History of Advertising Photography*. Harry N. Abrams, Inc.
- Solove, Daniel J. (2013). “Introduction: Privacy Self-Management and the Consent Dilemma.” *Harvard Law Review*. 126 (7): 1880-1903. <https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/>.
- Solove, Daniel J. (2023). “Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data.” 118 Northwestern University Law Review (forthcoming 2023). Available at SSRN: <https://ssrn.com/abstract=4322198> or <http://dx.doi.org/10.2139/ssrn.4322198>
- Solove, Daniel J., and Keats Citron, Danielle (2018). “Risk and Anxiety: A Theory of Data Breach Harms.” 96 Texas Law Review 737. <https://doi.org/10.2139/ssrn.2885638>.
- Spencer, Shaun B. (2020). “The Problem of Online Manipulation.” *University of Illinois Law Review* 3: 960–1006. <https://doi.org/10.2139/ssrn.3341653>.
- Spiekermann, Sarah, and Korunovska, Jana (2017). “Towards a Value Theory for Personal Data.” *Journal of Information Technology* 32 (1): 62–84. <https://doi.org/10.1057/jit.2016.4>.
- Stigler, George J. (1961). “The Economics of Information.” *The Journal of Political Economy* 69 (3): 213–25. <https://www.jstor.org/stable/1829263>.
- Strycharz, Joanna, and Duivenvoorde, Bram (2021). “The Exploitation of Vulnerability Through Personalised Marketing Communication: Are Consumers Protected?” *Internet Policy Review* 10 (4). <https://doi.org/10.14763/2021.4.1585>.
- Sunstein, Cass R (2016). *The Ethics of Influence*. Cambridge University Press.
- Sunstein, Cass R (2021). “Manipulation As Theft.” Harvard Public Law Working Paper No. 21-30, Available at SSRN: <https://ssrn.com/abstract=3880048> or <http://dx.doi.org/10.2139/ssrn.3880048>.
- Susser, Daniel, and Roessler, Beate and Nissenbaum, Helen F. (2019). “Online Manipulation: Hidden Influences in a Digital World.” *Georgetown Law Technology Review* 4 (1). <https://doi.org/10.2139/ssrn.3306006>.
- Sweeney, Latanya (2013) “Discrimination in Online Ad Delivery: Google Ads, Black Names and White Names, Racial Discrimination, and Click Advertising.” *Queue* 11 (3): 10–29. <https://queue.acm.org/detail.cfm?id=2460278>.
- Taleb, Nassim Nicholas (2013). *Antifragile: Things That Gain From Disorder*. London: Penguin.
- Taleb, Nassim Nicholas (2018). *Skin In The Game: Hidden Asymmetries in Daily Life*. New York: Random House.
- Teixeira, Thales, and Wedel, Michel and Pieters, Rik (2012). “Emotion-Induced Engagement in Internet Video Advertisements.” *Journal of Marketing Research* 49 (2): 144–59. <https://doi.org/10.1509/jmr.10.0207>.
- Tekbasan, Tolga (2019). “The Effects of Ad-Blocking on the Online Customer Behavior.” Master Thesis, University of Twente. <https://essay.utwente.nl/79763/>.
- Thaler, Richard H., and Sunstein, Cass R. (2021). *Nudge: The Final Edition*. Updated edition. New York: Penguin Books.
- Toen Vu, Hong and Saldaña, Magdalena (2021) “Chillin’ Effects of Fake News: Changes in Practices Related to Accountability and Transparency in American Newsrooms Under the Influence of Misinformation and Accusations Against the News Media”.

BIBLIOGRAPHY

- Journalism & Mass Communication Quarterly* 98(3): 769-789.
<https://journals.sagepub.com/doi/10.1177/1077699020984781>.
- Toubiana, Vincent, and Narayanan, Arvind and Boneh, Dan and Nissenbaum, Helen F. and Nissenbaum, Helen F. and Barocas, Solon. (2010) "Adnostic: Privacy Preserving Targeted Advertising", *Proceedings of the Network and Distributed System Symposium*, March 2010, Available at SSRN: <https://ssrn.com/abstract=2567076>.
- Trzaskowski, Jan (2021). *Your Privacy Is Important to US!* Ex København: Tuto Publishing.
- Turner, Ernest S. (1965). *The Shocking History of Advertising*. [Rev. ed.]. Penguin Book 2012. Harmondsworth, England: Penguin Books.
- Turow, Joseph (1998) *Breaking up America: Advertisers and The New Media World*. University of Chicago Press. <https://doi.org/10.1604/9780226817514>.
- Turow, Joseph (2017). *The Aisles Have Eyes : How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*. New Haven, Conn: Yale University Press.
- Tversky, Amos, and Kahneman, Daniel (1974). "Judgment under Uncertainty: Heuristics and Biases." *Science* 185 (4157): 1124-31.
<https://doi.org/10.1126/science.185.4157.1124>.
- Tversky, Amos, and Kahneman, Daniel (1986). "Rational Choice and the Framing of Decisions." *The Journal of Business* 59 (4): S251-78.
<https://www.jstor.org/stable/2352759>.
- van der Hof, Simone and Lievens, Eva (2017). "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR." *Communications Law* 23 (1). Available at SSRN: <https://ssrn.com/abstract=3107660>.
- van der Hof, Simone and Lievens, Eva and Milkaite, Ingrida and Verdoodt, Valerie, and Hannema, Thijs and Liefwaard, Tom (2020). "The Child's Right to Protection against Economic Exploitation in the Digital World in: The International Journal of Children's Rights" 28(4), 833-859. <https://doi.org/10.1163/15718182-28040003>.
- van der Hof, Simone, and van Hilten, Stijn and Ouburg, Sanne, and Birk, Max V. and van Rooij, Antonius J. (2022). "Don't Gamble With Children's Rights'-How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment." *Frontiers in Digital Health* 4: 822933.
<https://doi.org/10.3389/fdgth.2022.822933>.
- van der Wal, Goossen A. 1989. "The Individualism of Human Rights." *Rechtsfilosofie En Rechtstheorie* 18 (3): 195-206.
- van Santen, Esther (2022). "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*. Juho Mäkiö, Hochschule Emden/Leer (eds.).
http://personales.upv.es/thinkmind/ICCGI/ICCGI_2022/iccg_2022_1_20_18003.html.
- Varnali, Kaan (2021). "Online Behavioral Advertising: An Integrative Review." *Journal of Marketing Communications* 27 (1): 93-114.
<https://doi.org/10.1080/13527266.2019.1630664>.
- Veale, Michael, and Zuiderveen Borgesius, Frederik (2021). "Demystifying the Draft EU Artificial Intelligence Act." SocArXiv. <https://doi.org/10.31235/osf.io/38p5f>.
- Veale, Michael, and Zuiderveen Borgesius, Frederik (2022). "Adtech and Real-Time Bidding under European Data Protection Law." *German Law Journal* 23 (2): 226-56. <https://doi.org/10.1017/glj.2022.18>.
- Veale, Michael, Nouwens, Midas and Santos, Cristiana (2022). "Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the

BIBLIOGRAPHY

- Belgian DPA Decision?" *Technology and Regulation* 2022 (February): 12–22. <https://doi.org/10.26116/techreg.2022.002>.
- Verdoodt, Valerie, and Lievens, Eva (2017). "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*, 313–41. Maklu. <http://hdl.handle.net/1854/LU-8541057>.
- Vizard, Polly, and Fukuda-Parr, Sakiko and Elson, Diane (2011). "Introduction: The Capability Approach and Human Rights." *Journal of Human Development and Capabilities* 12 (1): 1–22. <https://doi.org/10.1080/19452829.2010.541728>.
- Vrabec, Helena U. (2019). "Uncontrollable: Data Subject Rights and the Data-Driven Economy." PhD Thesis. Leiden University. <https://hdl.handle.net/1887/68574>.
- Wachter, Sandra (2020). "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising." *Berkley Technology Law Journal* 35 (2). <https://doi.org/10.2139/ssrn.3388639>.
- Wachter, Sandra, and Mittelstadt, Brent (2019). "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review* 2019 (2): 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>.
- Walker, Margaret Urban (2013). "Moral Vulnerability and the Task of Reparations." In *Vulnerability: New Essays in Ethics and Feminist Philosophy*, by Catriona Mackenzie, Wendy Rogers, and Susan Dodds.
- Wallace, R. Jay (2020) "Practical Reason." The Stanford Encyclopedia of Philosophy (Spring 2020 Edition), Edward N. Zalta (ed.), <https://plato.stanford.edu/archives/spr2020/entries/practical-reason/> (accessed November 2, 2023)..
- Warren, Samuel D. and Brandeis, Louis D. (1890). "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220. <https://doi.org/10.2307/1321160>.
- Weiser, Mark (1991). "The Computer for the 21 St Century." *Scientific American* 265 (3): 94–105. <https://doi.org/10.1145/329124.329126>.
- Westin, Alan (1967). *Privacy And Freedom*. New York: Ig Publishing.
- White, Ryen W. and Doraiswamy, P. Murali and Horvitz, Eric (2018). "Detecting Neurodegenerative Disorders from Web Search Signals." *NPJ Digital Medicine* 1 (April): 8. <https://doi.org/10.1038/s41746-018-0016-6>.
- Whittington, Jan and Hoofnagle, Chris Jay (2012). "Unpacking Privacy's Price." *The North Carolina Law Review* 90 (1327).
- Wood, Allen W (2014). "Coercion, Manipulation, Exploitation." In *Manipulation: Theory and Practice*, 17-50, Christian Coons and Michael Weber (eds.), Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199338207.003.0002>.
- Wu, Tim (2011). *The Master Switch: The Rise and Fall of Information Empires*. New York: Knopf.
- Wu, Tim (2016). *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. New York: Knopf.
- Yeung, Karen (2016). "'Hypernudge': Big Data as a Mode of Regulation by Design." *Information, Communication & Society* 20 (May): 1–19. <https://doi.org/10.1080/1369118X.2016.1186713>.
- Zard, Lex, and Fosch-Villaronga, Eduard (2020). "'Oh, Dignity Too?' Said the Robot: Human Dignity as the Basis for the Governance of Robotics." *Minds and Machines* 30 (1): 121–43. <https://doi.org/10.1007/s11023-019-09514-6>.
- Zard, Lex, and Sears, Alan M. (2023). "Targeted Advertising and Consumer Protection Law in the European Union." *Vanderbilt Journal of Transnational Law* 56 (559): 795–848.

BIBLIOGRAPHY

- Zarsky, Tal (2017). "Incompatible: The GDPR in the Age of Big Data." *Seton Hall Law Review* 47 (4). <https://scholarship.shu.edu/shlr/vol47/iss4/2>.
- Zarsky, Tal (2019). "Privacy and Manipulation in the Digital Age." *Theoretical Inquiries in Law* 20 (1). <https://www7.tau.ac.il/ojs/index.php/til/article/view/1612>.
- Zhang, Kaifu, and Katona, Zsolt (2012). "Contextual Advertising." *Marketing Science* 31 (6): 980–94. <https://doi.org/10.1287/mksc.1120.0740>.
- Zimmeck, Sebastian, and Li, Jie S. and Kim, Hyungtae and Bellovin, Steven M. and Jebara, Tony (2017). "A Privacy Analysis of Cross-Device Tracking." In *Open Access to the Proceedings of the 26th USENIX Security Symposium Is Sponsored by USENIX*. <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/zimmeck>.
- Zittrain, Jonathan (2006). "A History of Online Gatekeeping." *Harvard Journal of Law and Technology* 19 (253). <http://nrs.harvard.edu/urn-3:HUL.InstRepos:4455491>.
- Zuboff, Shoshana (2015). "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75-89 <https://doi-org.ezproxy.leidenuniv.nl/10.1057/jit.2015.5>.
- Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight For A Human Future at The New Frontier of Power*. First edition. New York: PublicAffairs.
- Zuboff, Shoshana (2022). "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization." *Organization Theory*, 3(3). <https://doi-org.ezproxy.leidenuniv.nl/10.1177/26317877221129290>.
- Zuiderveen Borgesius, Frederik J. (2013). "Consent to Behavioural Targeting in European Law - What Are Policy Implications of Insights from Behavioural Economics?" Amsterdam Law School Legal Studies Research Paper No. 2013-43. Available at SSRN: <https://ssrn.com/abstract=2300969> or <http://dx.doi.org/10.2139/ssrn.2300969>.
- Zuiderveen Borgesius, Frederik J. (2015). "Personal Data Processing for Behavioural Targeting: Which Legal Basis?" *International Data Privacy Law* 5 (3). <https://academic.oup.com/idpl/article/5/3/163/730611>.
- Zuiderveen Borgesius, Frederik J. (2015). *Improving Privacy Protection in the Area of Behavioral Targeting*. Information Law Series 33. Kluwer Law International.
- Zuiderveen Borgesius, Frederik J. (2016). "Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation." *Computer Law & Security Review* 32 (2): 256–71. <https://doi.org/10.1016/j.clsr.2015.12.013>.
- Zuiderveen Borgesius, Frederik, and Poort, Joost (2017). "Online Price Discrimination and EU Data Privacy Law." *Journal of Consumer Policy* 40 (3): 347–66. <https://doi.org/10.1007/s10603-017-9354-z>.

Online Sources

News Articles and Blog Posts

- Bertuzzi, Luca (February 28, 2023). "EU Policymakers Have Adtech in Sight for Future Regulation." IAPP. <https://iapp.org/news/a/eu-policymakers-have-adtech-in-sight-for-future-regulation/> (accessed October 4, 2023).
- Bertuzzi, Luca (May, 11, 2023). "AI Act Moves Ahead in EU Parliament with Key Committee Vote." EURACTIV. <https://www.euractiv.com/section/artificial->

BIBLIOGRAPHY

- [intelligence/news/ai-act-moves-ahead-in-eu-parliament-with-key-committee-vote/](#) (accessed November 2, 2023).
- Birch, Jacey* (February 28, 2023). “Social Media Now Having Influence on Pet Adoptions.” LOCAL10.COM. <https://www.local10.com/news/local/2023/02/28/social-media-now-having-influence-on-pet-adoptions/> (accessed November 2, 2023).
- Bohn, Dieter* (June 24, 2021). “Google Chrome Third-Party Cookies Block Delayed Until 2023.” THE VERGE. <https://www.theverge.com/2021/6/24/22547339/google-chrome-cookiepocalypse-delayed-2023> (accessed January 5, 2023).
- Burgess, Kaya* (August 3, 2018). “Teacup Dogs Have Big Health Problems,” THE TIMES. <https://www.thetimes.co.uk/article/teacup-dogs-have-big-health-problems-t3zvzmtnd> (accessed November 2, 2023).
- Burgess, Matt* (January 27, 2022). “Google Has a New Plan to Kill Cookies. People Are Still Mad.” WIRED. <https://www.wired.com/story/google-floc-cookies-chrome-topics/> (accessed January 5, 2023).
- Chavez, Anthony* (July 27, 2022). “Expanding Testing for the Privacy Sandbox for the Web.” GOOGLE: THE KEYWORD. <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> (accessed November 2, 2023).
- Chee, Foo Yun* (July 5, 2023). “Meta Loses as Top EU Court Backs Antitrust Regulators over Privacy Breach Checks.” REUTERS. <https://www.reuters.com/technology/german-antitrust-watchdog-can-add-privacy-breaches-meta-probe-eu-court-says-2023-07-04/> (accessed November 2, 2023).
- Chen, Brian X.* (December 2, 2008). “Apple: Our Ads Don’t Lie, But You’re a Fool If You Believe Them.” WIRED. <https://www.wired.com/2008/12/apple-says-cust/> (accessed November 2, 2023).
- Clasen, Aline* (April 12, 2023). “Austria Challenges EU Newspapers’ Pay-or-Cookie Walls.” 2023. EURACTIV. <https://www.euractiv.com/section/media/news/austria-challenges-eu-newspapers-pay-or-cookie-walls/> (accessed October 31, 2023).
- Crawford, Angus and Bell, Bethan* (September 30, 2022). “Molly Russell Inquest: Father Makes Social Media Plea,” BBC NEWS. <https://www.bbc.com/news/uk-england-london-63073489> (accessed October 31, 2023).
- Cross, Tim* (May 16, 2023). “IAB Removes Legitimate Interest from Reworked TCF.” VIDEOWEEK. <https://videoweek.com/2023/05/16/iab-removes-legitimate-interest-from-reworked-tcf/> (accessed November 2, 2023).
- da Rosa Lazarotto, Bárbara and Malgieri, Gianclaudio* (May 4, 2023). “The Data Act: A (Slippery) Third Way Beyond Personal/Non-Personal Data Dualism?” EUROPEAN LAW BLOG. <https://europeanlawblog.eu/2023/05/04/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/> (accessed November 2, 2023).
- Davies, Jessica* (January 16, 2019). “After GDPR, The New York Times Cut off Ad Exchanges in Europe -- and Kept Growing Ad Revenue.” DIGIDAY. <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/> (accessed November 2, 2023).
- Derudder, Kimberley* (October 26, 2021). “What Is The Environmental Footprint For Social Media Applications? 2021 Edition.” GREENSPECTOR. <https://greenspector.com/en/social-media-2021/> (accessed November 2, 2023).
- Dodgson, Lindsay* (July 26, 2022). “Why TikTok Makes the Hours Seem to Melt Away, According to Experts Who Study How Our Brains Perceive Time.” INSIDER. <https://www.insider.com/why-time-passes-so-quickly-scrolling-on-tiktok-2022-7> (accessed April 10, 2023).
- Duhigg, Charles* (February 16, 2012). “How Companies Learn Your Secrets.” THE NEW YORK TIMES, <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html> (accessed November 2, 2023).

BIBLIOGRAPHY

- Dumitrascu, Mihnea* (March 28, 2023). “DSA - Targeted Advertising Aimed at Minors: A Future Ban?” BIRD & BIRD. <https://www.twobirds.com/en/insights/2023/global/dsa-publicite-ciblee-destinee-aux-mineurs-une-interdiction-a-venir> (accessed May 8, 2023).
- Eagle, James* (September 9, 2022). “Animation: The Most Popular Websites by Web Traffic (1993-2022).” VISUAL CAPITALIST. <https://www.visualcapitalist.com/cp/most-popular-websites-by-web-traffic/> (accessed November 2, 2023).
- Edelman, Gilad* (March 22, 2020). “Why Don’t We Just Ban Targeted Advertising?” WIRED, 2020. <https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/> (accessed November 2, 2023).
- Erickson, D’arcy/McCaan* (February 1, 2012). “The History of Coca-Cola’s It’s the Real Thing Sogan.” CREATIVE REVIEW. <https://www.creativereview.co.uk/its-the-real-thing-coca-cola/> (accessed November 2, 2023).
- Felicity, Thea* (May 8, 2022). “Top 5 Best Consent Management Platforms in 2022 To Easily and Legally Manage User Data.” TECHTIMES. <https://www.techtimes.com/articles/272671/20220308/top-5-best-consent-management-platforms-in-2022-to-easily-and-legally-manage-user-data.htm> (accessed November 2, 2023).
- Forester* (September 4, 2019) “Google, Facebook, and Amazon: From Duopoly To Triopoly of Advertising.” Forbes. <https://www.forbes.com/sites/forrester/2019/09/04/google-facebook-and-amazon-from-duopoly-to-triopoly-of-advertising/?sh=6ae96ead6343> (accessed January 4, 2023.)
- Franklin, Matija, and Ashton, Hal and Gorman, Rebecca and Armstrong, Stuart* (March, 21 2023). “The EU’s AI Act Needs to Address Critical Manipulation Methods.” OECD.AI POLICY OBSERVATORY. <https://oecd.ai/en/wonk/ai-act-manipulation-methods> (accessed November 2, 2023).
- Goujard, Clothilde* (January 13, 2022). “CEOs Make Final Push to Ban Targeted Ads.” 2022. POLITICO. <https://www.politico.eu/article/activist-ceo-mep-crack-down-targeted-ads-vote-digital-services-act-2/> (accessed October 31, 2023).
- Greene, Diane* (June 23, 2017). “As G Suite Gains Traction in the Enterprise, G Suite’s Gmail and Consumer Gmail to More Closely Align.” GOOGLE: THE KEYWORD. <https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/> (accessed October 31, 2023).
- Hackett, Robert* (November 18, 2019). “Harvard Economist Calls to Outlaw Online Advertising Markets—Just Like ‘Organs, Babies, or Slaves.’” FORTUNE. <https://fortune.com/2019/11/18/google-facebook-online-advertising-ban-surveillance-capitalism/> (accessed November 2, 2023).
- Hansell, Saul* (April 8, 2002). “Google’s Toughest Search Is for a Business Model.” THE NEW YORK TIMES. <https://www.nytimes.com/2002/04/08/business/google-s-toughest-search-is-for-a-business-model.html> (accessed November 2, 2023).
- Hansen, Royal* (February 1, 2023). “How We Achieve Privacy through Innovation.” GOOGLE. <https://blog.google/technology/safety-security/how-we-achieve-privacy-through-innovation/> (accessed November 2, 2023).
- Häuselmann, Andreas* (February 20, 2023). “The ECJ’s First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber.” EUROPEAN LAW BLOG. <https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/> (accessed November 2, 2023).
- Hern, Alex, and Ledegaard, Frederik Hugo* (October 9, 2019). “Children ‘interested in’ Gambling and Alcohol, According to Facebook.” THE GUARDIAN.

BIBLIOGRAPHY

- <https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook> (accessed November 2, 2023).
- Hill, Kashmir* (February 16, 2012). “How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.” FORBES. <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> (accessed January 2, 2023).
- Ikeda, Scott* (May 24, 2022). “Report on RTB: Adtech ‘Biggest Data Breach Ever Recorded,’ Online Behavior More Exposed in Countries Without Privacy Regulations.” CPO MAGAZINE. <https://www.cpomagazine.com/data-privacy/report-on-rtb-adtech-biggest-data-breach-ever-recorded-online-behavior-more-exposed-in-countries-without-privacy-regulations/> (accessed November 2, 2023).
- Isaac, Mike, and Hsu, Tiffany* (November 9, 2021). “Meta Plans to Remove Thousands of Sensitive Ad-Targeting Categories.” THE NEW YORK TIMES. <https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html> (accessed November 2, 2023).
- Kahn, Robert and Dennis, Michael Aaron* (October 10, 2023) “Internet: Description, History, Uses, & Facts.” BRITANNICA. <https://www.britannica.com/technology/Internet> (accessed January 17, 2023).
- Koren, Marina* (March 20, 2013). “B.F. Skinner: The Man Who Taught Pigeons to Play Ping-Pong and Rats to Pull Levers.” SMITHSONIAN MAGAZINE. <https://www.smithsonianmag.com/science-nature/bf-skinner-the-man-who-taught-pigeons-to-play-ping-pong-and-rats-to-pull-levers-5363946/> (accessed March 20, 2023).
- Lomas, Natasha* (January 20, 2019). “The Case Against Behavioral Advertising Is Stacking Up.” TECHCRUNCH. <https://techcrunch.com/2019/01/20/dont-be-creepy/> (accessed November 2, 2023).
- Lomas, Natasha* (July 4, 2023). “CJEU Ruling on Meta Referral Could Close the Chapter on Surveillance Capitalism,” TECHCRUNCH. <https://techcrunch.com/2023/07/04/cjeu-meta-superprofiling-decision/> (accessed November 2, 2023).
- Loveless, Jacob* (August 22, 2022). “Council Post: How Does Apple’s App Tracking Transparency Framework Affect Advertisers?” FORBES. <https://www.forbes.com/sites/forbesbusinesscouncil/2022/08/22/how-does-apples-app-tracking-transparency-framework-affect-advertisers/> (accessed January 5, 2023).
- Machkovech, Sam* (May 1, 2017). “Report: Facebook Helped Advertisers Target Teens Who Feel ‘Worthless’ [Updated].” ARS TECHNICA. <https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/> (accessed March 3, 2023).
- MacMillan, Douglas* (July 2, 2018). “Tech’s ‘Dirty Secret’: The App Developers Sifting Through Your Gmail.” WALL STREET JOURNAL. <https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442> (accessed November 2, 2023).
- Mathews, Lee* (April 17, 2019). “A Dangerous Flaw In Popular Ad Blockers Put 100 Million Users At Risk.” FORBES <https://www.forbes.com/sites/leemathews/2019/04/17/a-dangerous-flaw-in-popular-ad-blockers-put-100-million-users-at-risk/> (accessed November 2, 2023).
- McDonald Ellis, Magee John* (November 27, 2020). “European Law on Cookies.” DLA PIPER. <https://www.dlapiper.com/en-gb/insights/publications/2020/11/european-law-on-cookies> (accessed January 5, 2023).

BIBLIOGRAPHY

- Moser, Katie* (May 11, 2023). "How to Personalize Content Using First Party Cookies and Data." ZESTY. <https://www.zesty.io/mindshare/how-to-personalize-content-using-first-party-cookies-and-data/> (accessed January 4, 2023).
- Newman, Daniel* (February 10, 2022). "Apple, Meta And The \$10 Billion Impact Of Privacy Changes." FORBES. <https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/> (accessed November 2, 2023).
- Newton, Casey* (January 18, 2018). "'Time Well Spent' Is Shaping up to Be Tech's next Big Debate." THE VERGE. <https://www.theverge.com/2018/1/17/16903844/time-well-spent-facebook-tristan-harris-mark-zuckerberg> (accessed November 2, 2023).
- Nunes, Ciao* (July 7, 2023). "CJEU Lands Groundbreaking Decision on Data Protection and Antitrust." LEXOLOGY. TREVISAN & CUONZO. <https://www.lexology.com/library/detail.aspx?g=e722bd9d-5135-4536-90aa-5b58c4a268d7> (accessed November 2, 2023).
- Oehlschlager, Mie* (October 19, 2020). "Open Letter: Children Are Subjected To Behavioural Advertising - End It!" *Dataetisk Tænkehandlebank*. <https://dataethics.eu/open-letter-children-are-subjected-to-behavioural-advertising-end-it/> (accessed November 2, 2023).
- Poulsen, Kevin* (February, 10 2019). "Inside the Secret Facebook War For Mormon Hearts and Minds." THE DAILY BEAST. <https://www.thedailybeast.com/inside-the-secret-facebook-war-for-mormon-hearts-and-minds> (accessed November 2, 2023).
- Qayyah, Asenjo and Moynihan, Alba* (2019). "Facebook Quietly Ditched the 'It's Free and Always Will Be' Slogan From Its Homepage." BUSINESS INSIDER. <https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8> (accessed November 2, 2023).
- Rijks Maarten* (September 19, 2022). "The DSA: Advertising, Dark Patterns and Recommender Systems." TAYLORWESING. <https://www.taylorwessing.com/en/interface/2022/the-eus-digital-services-act/the-dsa-advertising-dark-patterns-and-recommender-systems> (accessed November 2, 2023).
- Ritchie, Hannah, and Roser, Max and Rosado, Pablo* (2020). "Netherlands: CO₂ Country Profile." OUR WORLD IN DATA. <https://ourworldindata.org/co2/country/netherlands> (accessed November 2, 2023).
- Rosen, Rebecca J.* (October 3, 2013). "Is This the Grossest Advertising Strategy of All Time?" THE ATLANTIC. <https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/> (accessed November 2, 2023).
- Ryan, Johnny* (May 24, 2023). "Don't Be Fooled By Meta's Fine For Data Breaches, Says Johnny Ryan." THE ECONOMIST. <https://www.economist.com/by-invitation/2023/05/24/dont-be-fooled-by-metas-fine-for-data-breaches-says-johnny-ryan> (accessed May 30, 2023).
- Sattiraju, Nikitha* (April 2, 2020). "Secret Cost of Google's Data Centers: Billions of Gallons of Water." TIME. <https://time.com/5814276/google-data-centers-water/> (accessed November 2, 2023).
- Schechner, Sam* (October 3, 2023). "Meta Plans to Charge \$14 a Month for Ad-Free Instagram or Facebook." WALL STREET JOURNAL. <https://www.wsj.com/tech/meta-floats-charging-14-a-month-for-ad-free-instagram-or-facebook-5dbaf4d5> (accessed November 2, 2023).
- Schiffman, Betsy* (December 4, 2007). "Facebook Is Always Watching You." WIRED. <https://www.wired.com/2007/12/facebooks-is-al/> (accessed November 2, 2023).

BIBLIOGRAPHY

- Schwartz, John* (September 4, 2001). "Giving Web a Memory Cost Its Users Privacy." THE NEW YORK TIMES. <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> (accessed November 2, 2023).
- Shellenbarger, Sue* (November 21, 2016). "Most Students Don't Know When News Is Fake, Stanford Study Finds." WALL STREET JOURNAL. <https://www.wsj.com/articles/most-students-dont-know-when-news-is-fake-stanford-study-finds-1479752576> (accessed April 10, 2023).
- Shields, Ronan* (December 13, 2022). "Here Are the 2022 Global Media Rankings by Ad Spend: Google, Facebook Remain Dominant -- Alibaba, ByteDance in the Mix." DIGIDAY. <https://digiday.com/media/the-rundown-here-are-the-2022-global-media-rankings-by-ad-spend-google-facebook-remain-dominant-alibaba-bytedance-in-the-mix/> (accessed November 2, 2023).
- Silverman, Ryan and Mac, Craig* (January 14, 2021). "Facebook Has Been Showing Military Gear Next To Insurrection Posts." BUZZFEED NEWS. <https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot> (accessed November 2, 2023).
- Statt, Nick* (March 24, 2020). "Apple Updates Safari's Anti-Tracking Tech With Full Third-Party Cookie Blocking." THE VERGE. <https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking> (accessed January 5, 2023).
- Valentino-DeVries, Jennifer, and Singer-Vine, Jeremy and Soltani, Ashkan* (December 24, 2012). "Websites Vary Prices, Deals Based on Users' Information." WALL STREET JOURNAL. <https://online.wsj.com/article/SB10001424127887323777204578189391813881534.html> (accessed November 2, 2023).
- Varese, Elena* (November 29, 2021). "Animal Welfare and the Depiction of Animals in Advertising." DLA PIPER. <https://www.dlapiper.com/en-sg/insights/publications/2021/11/animal-welfare-and-the-depiction-of-animals-in-advertising> (accessed October 31, 2023).
- Wickramasinghe, Shanika and Zoltan, Miklos* (July 9, 2022). "A Complete Guide To Google FLoC - What It Does and How It Works - How FloC Affects Privacy," PRIVACY AFFAIRS. <https://www.privacyaffairs.com/google-floc/> (accessed October 31, 2023).
- Wood, Marissa* (September 3, 2019). "Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default." DIST://ED. <https://blog.mozilla.org/en/products/firefox/firefox-news/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/> (accessed January 5, 2023.)
- Yonego, Joris Toonders* (July 23, 2014). "Data Is the New Oil of the Digital Economy." WIRED, July 23, 2014. <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> (accessed November 2, 2023).

Web Recourses

- "'Pay or Okay' on Tech News Site Heise.de Illegal, Decides German DPA." NOYB (July 14, 2023). <https://noyb.eu/en/pay-or-okay-tech-news-site-heisede-illegal-decides-german-dpa> (accessed October 31, 2023).
- "10 Evil Vintage Cigarette Ads Promising Better Health." Healthcare Administration Degree Programs. (April 16, 2013). <https://www.healthcare-administration-degree.net/10-evil-vintage-cigarette-ads-promising-better-health/> (accessed November 2, 2023).

BIBLIOGRAPHY

- “About Audience Targeting.” GOOGLE ADS HELP. Accessed October 31, 2023. <https://support.google.com/google-ads/answer/2497941?hl=en>.
- “About Demographic Targeting.” GOOGLE ADS HELP. Accessed January 2, 2023. <https://support.google.com/google-ads/answer/2580383>.
- “About Detailed Targeting.” META BUSINESS HELP CENTER. Accessed January 3, 2023. <https://www.facebook.com/business/help/182371508761821>.
- “About Lookalike Audiences.” META BUSINESS HELP CENTER. Accessed January 3, 2023. <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.
- “About Quality Score.” GOOGLE ADS HELP. Accessed January 3, 2023. <https://support.google.com/google-ads/answer/6167118?hl=en>.
- “About Similar Segments for Search.” GOOGLE ADS HELP. Accessed January 3, 2023. <https://support.google.com/google-ads/answer/7151628>.
- “Ad Selection White Paper.” GOOGLE AD MANAGER HELP. Accessed January 5, 2023. <https://support.google.com/admanager/answer/1143651>.
- “AdBlock VPN: Get It Now.” ADBLOCK VPN. Accessed March 30, 2023. <https://vpn.getadblock.com/en/purchase/>.
- “AdChoices for the Google Display Network.” GOOGLE AD MANAGER. Accessed March 1, 2023. <https://support.google.com/admanager/answer/2695279?hl=en#zippy=%2Cexample-in-display-ads%2Cexample-in-video-ads>.
- “Adnostic: Privacy Preserving Targeted Advertising.” ADNOSTIC. Accessed January 19, 2023. <https://crypto.stanford.edu/adnostic/>.
- “Advertising the Model T.” THE HENRY FORD BLOG. Accessed January 18, 2023. <https://www.thehenryford.org/explore/blog/advertising-the-model-t/>.
- “Advertising with Google Ad Manager.” GOOGLE AD MANAGER HELP. Accessed January 5, 2023. <https://support.google.com/admanager/answer/6022000?hl=en>.
- “Alphabet.” ALPHABET. Accessed October 10, 2022. <https://abc.xyz/>.
- “Apple Media Services Terms and Conditions.” APPLE LEGAL. Accessed November 15, 2022. <https://www.apple.com/legal/internet-services/itunes/us/terms.html>.
- “Authorized Buyers Real-Time Bidding Proto.” GOOGLE DEVELOPERS. Accessed January 5, 2023. <https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide>.
- “Ban Surveillance Advertising.” BAN SURVEILLANCE ADVERTISING. Accessed May 6, 2023. <https://www.bansurveillanceadvertising.com/>.
- “Big Data Is Watching You.” CORPORATE EUROPE OBSERVATORY. (October 17, 2017). <https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you> (accessed November 2, 2023).
- “BREAKING: Meta Prohibited from Use of Personal Data for Advertising.” NOYB. January 4, 2023. <https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising> (accessed November 2, 2023).
- “Browser Market Share Worldwide.” STATCOUNTER GLOBAL STATS. Accessed January 5, 2023. <https://gs.statcounter.com/browser-market-share>.
- “Clickthrough Rate (CTR): Definition.” GOOGLE ADS HELP. Accessed January 4, 2023. https://support.google.com/google-ads/answer/2615875?hl=en&ref_topic=24937.
- “Commerce Ranking Disclosure.” FACEBOOK. Accessed January 3, 2023. https://www.facebook.com/legal/commerce_ranking.
- “Consent Management, Cookie Consent According to EU GDPR.” CIDAAS. Accessed February 27, 2023. <https://www.cidaas.com/consent-management/#:~:text=Cookie%20Management&text=According%20to%20the%20EU's%20e.%2Dcalled%20opt%2Din%20procedure>.
- “Contextual Targeting.” GOOGLE ADS HELP. Accessed January 2, 2023. <https://support.google.com/google-ads/answer/1726458?hl=en>.

BIBLIOGRAPHY

- “Cookie walls : la CNIL publie des premiers critères d’évaluation.” CNIL (May 16, 2022). <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation>.
- “Cover Your Tracks.” ELECTRONIC FRONTIER FOUNDATION. Accessed January 19, 2023. <https://coveryourtracks EFF.org/learn>.
- “Craigslist: Amsterdam.” CRAIGSLIST. Accessed January 11, 2023. <https://amsterdam.craigslist.org>.
- “Critics Pan Google-DoubleClick Ruling.” POLITICO (March 18, 2008). <https://www.politico.eu/article/critics-pan-google-doubleclick-ruling/> (accessed November 2, 2023).
- “Cybersecurity Vulnerabilities: Types, Examples, and More.” GREAT LEARNING. (August 14, 2023). <https://www.mygreatlearning.com/blog/cybersecurity-vulnerabilities/> (accessed November 2, 2023).
- “Data Privacy Act: A Brief History of Modern Data Privacy Laws.” EPERI. (2018). <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws> (accessed November 2, 2023).
- “Definition of Vulnerable.” MERRIAM-WEBSTER. Accessed January 17, 2023. <https://www.merriam-webster.com/dictionary/vulnerable>.
- “Digital Advertising - Europe.” STATISTA. Accessed May 2, 2023. <https://www.statista.com/outlook/dmo/digital-advertising/europe>.
- “Digital Services Act: How Does It Protect Animals From The Illegal Online Trade?” EUROGROUPFORANIMALS. Accessed April 10, 2023. <https://www.eurogroupforanimals.org/news/digital-services-act-how-does-it-protect-animals-illegal-online-trade>.
- “Embed Videos & Playlists.” YOUTUBE HELP. Accessed January 19, 2023. <https://support.google.com/youtube/answer/171780?hl=en>.
- “Estimate Your Results with Bid, Budget and Target Simulators.” GOOGLE ADS HELP. Accessed January 4, 2023. https://support.google.com/google-ads/answer/2470105?hl=en&ref_topic=3122864.
- “EU Audiovisual and Media Policies.” EUROPEAN COMMISSION. Accessed July 17, 2023. https://ec.europa.eu/archives/information_society/avpolicy/reg/tvwf/provisions/scop e/index_en.htm.
- “EU: Put Fundamental Rights at Top of Digital Regulation.” (January 7, 2022). HUMAN RIGHTS WATCH. <https://www.hrw.org/news/2022/01/07/eu-put-fundamental-rights-top-digital-regulation> (accessed November 2, 2023).
- “EUR-Lex.” An Official Website of the European Union. Accessed November 29, 2022. <https://eur-lex.europa.eu/homepage.html>.
- “Explore Advanced Advertising Strategies.” GOOGLE ADS. Accessed June 9, 2023. https://ads.google.com/intl/en_ie/home/resources/advanced/.
- “Facebook Does Not Make the Laws! S&Ds Launch Pan-European Campaign To Stop Online Data Abuse.” SOCIALISTS & DEMOCRATS (February 23, 2021). <https://www.socialistsanddemocrats.eu/newsroom/facebook-does-not-make-laws-sds-launch-pan-european-campaign-stop-online-data-abuse> (accessed November 2, 2023).
- “Federated Learning of Cohorts (FLoC).” GOOGLE THE PRIVACY SANDBOX. Accessed January 19, 2023. <https://privacysandbox.com/proposals/floc/>.
- “Global Daily Social Media Usage 2022.” STATISTA. Accessed March 29, 2023. <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/>.
- “Glossary of Terminology.” IAB. Accessed January 3, 2023. <https://www.iab.com/insights/glossary-of-terminology/>.

BIBLIOGRAPHY

- “Google and IAB TCF v2.2: How Publishers Can Stay Ahead with CookieYes.” COOKIEYES. (August 22, 2023). <https://www.cookieyes.com/blog/iab-tcf-cmp-for-publishers/> (accessed June 2, 2023).
- “Google Mission.” GOOGLE SEARCH. Accessed February 23, 2023. <https://www.google.com/search/howsearchworks/our-approach/>
- “Google Revenue 2002-2022.” STATISTA. Accessed April 23, 2023. <https://www.statista.com/statistics/266206/googles-annual-global-revenue/>.
- “History of Advertising.” WIKIPEDIA. Accessed January 4, 2023 https://en.wikipedia.org/wiki/History_of_advertising.
- “How Online Ads Discriminate: Unequal Harms of Online Advertising in Europe.” EUROPEAN DIGITAL RIGHTS (EDRI). Accessed November 2, 2023. <https://edri.org/our-work/how-online-ads-discriminate/>.
- “How the European Parliament’s Proposals on Surveillance Advertising Changed Over Time,” CORPORATE EUROPE OBSERVATORY (January 18, 2022). <https://corporateeurope.org/en/2022/01/how-corporate-lobbying-undermined-eus-push-ban-surveillance-ads> (accessed October 31, 2023).
- “How to Sell on Amazon.” AMAZON. Accessed November 15, 2022. <https://sell.amazon.com/sell>.
- “How We Make Money with Advertising.” GOOGLE. Accessed November 15, 2022. <https://howwemakemoney.withgoogle.com>.
- “HTTP Cookie.” WIKIPEDIA. Accessed November 2, 2023. https://en.wikipedia.org/wiki/HTTP_cookie.
- “HUDOC.” EUROPEAN COURT OF HUMAN RIGHTS. Accessed November 2, 2023. <https://hudoc.echr.coe.int>.
- “IAB Europe Seeks Court Decision on Validation Of The Action Plan as It Moves Forward With TCF Evolutions.” IAB EUROPE. (February 10, 2023). <https://iabeurope.eu/all-news/iab-europe-seeks-court-decision-on-validation-of-the-action-plan-as-it-moves-forward-with-tcf-evolutions/>. (Accessed May 4, 2023).
- “Introducing Campaign Manager 360.” CAMPAIGN MANAGER 360 HELP. Accessed January 5, 2023. <https://support.google.com/campaignmanager/answer/10157783?hl=en>.
- “Introducing Meta: A Social Technology Company.” META. (October 28, 2021). <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> (accessed November 2, 2023).
- “Introducing New Ways to Verify Age on Instagram.” META. (June 23, 2022). <https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/>. (accessed November 2, 2023).
- “Largest Companies by Market Cap.” COMPANIESMARKETCAP. Accessed October 10, 2022. <https://companiesmarketcap.com/>.
- “Largest Global Advertisers 2021.” STATISTA. Accessed January 12, 2023. <https://www.statista.com/statistics/286448/largest-global-advertisers/>.
- “Laura Moy & Amanda Conley, Paying the Wealthy for Being Wealthy: The Hidden Costs of Behavioral Marketing.” BERKELEY LAW. (May 24, 2013). <https://sites.law.berkeley.edu/privacylaw/2013/05/24/laura-moy-amanda-conley-paying-the-wealthy-for-being-wealthy-the-hidden-costs-of-behavioral-marketing/> (accessed March 27, 2023).
- “Ledger of Harms.” CENTER FOR HUMANE TECHNOLOGY. (June 2021). <https://ledger.humanetech.com/> (accessed November 2, 2023).
- “Lingchi.” WIKIPEDIA. Accessed April 12, 2023. <https://en.wikipedia.org/wiki/Lingchi>.
- “Manipulate.” BRITANNICA DICTIONARY. Accessed January 24, 2023. <https://www.britannica.com/dictionary/manipulate>.
- “MediaMath.” MEDIAMATH. Accessed January 18, 2023. <https://www.mediamath.com/>.

BIBLIOGRAPHY

- “Meta Audience Network.” META. Accessed June 9, 2023. <https://www.facebook.com/audiencenetwork/>.
- “Meta: Annual Revenue and Net Income 2022.” STATISTA. 2023. Accessed November 2, 2023 <https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/>.
- “Methods and Apparatus for Ordering Advertisements Based on Performance Information.” US Patent US20160162931A1, filed: March 29, 2002, by Georges Harik, Lawrence Page, and Jane Manning. Issued. June 9, 2016. Accessed November 2, 2023. <https://patents.google.com/patent/US20160162931A1/en?q=~patent%2fUS9152718B2&q=G06Q30%2f0254>.
- “More Cookie Banners to Go: Second Wave of Complaints Underway.” NOYB. (March 4, 2022). <https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway> (accessed March 30, 2023).
- “Most Visited Websites - Top Websites Ranking for December 2022.” SIMILARWEB. Accessed January 12, 2023. <https://www.similarweb.com/top-websites/>.
- “Netflix Terms of Use.” NETFLIX. Accessed January 12, 2023. <https://help.netflix.com/legal/termsfuse>.
- “Noyb.Eu Filed Complaints over ‘Forced Consent’ against Google, Instagram, WhatsApp and Facebook.” NOYB. (May 25, 2018). <https://noyb.eu/en/noybeu-filed-complaints-over-forced-consent-against-google-instagram-whatsapp-and-facebook> (accessed May 2, 2023).
- “On Interests and Values” MAASTRICHT UNIVERSITY LAW BLOG (September 6, 2019). <https://www.maastrichtuniversity.nl/blog/2019/09/interests-and-values> (accessed July 3, 2023).
- “OpenRTB (Real-Time Bidding).” IAB TECH LAB. Accessed January 19, 2023. <https://iabtechlab.com/standards/openrtb/>.
- “OpenRTB Integration.” GOOGLE DEVELOPERS. Accessed January 5, 2023. <https://developers.google.com/authorized-buyers/rtb/openrtb-guide>.
- “Personalized Advertising.” GOOGLE ADVERTISING POLICIES HELP. Accessed January 2, 2023. <https://support.google.com/adspolicy/answer/143465?hl=en>.
- “Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail.” PRIVACYRIGHTS.ORG. Accessed February 27, 2023. <https://privacyrights.org/resources/privacy-and-civil-liberties-organizations-urge-google-suspend-gmail>.
- “Privacy Zuckering: Deceiving Your Privacy by Design.” MEDIUM. (April 10, 2017). <https://medium.com/@mohityadav0493/privacy-zuckering-deceiving-your-privacy-by-design-d41b6263b564> (accessed November 2, 2023).
- “Publisher Platforms.” XANDR. Accessed January 18, 2023. <https://www.xandr.com/solutions/monetize/>.
- “Quackery.” 2023. BRITANNICA. Accessed January 17, 2023. <https://www.britannica.com/topic/quackery>.
- “Quantcast Choice Powers One Billion Consumer Consent Choices in Two Months Since GDPR.” QUANTCAST. (July 30, 2018). <https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/> (accessed February 27, 2023).
- “reCAPTCHA: Easy on Humans, Hard on Bots.” GOOGLE RECAPTCHA. Accessed February 23, 2023. <https://www.google.com/recaptcha/intro/?hl=es/index.html>.
- “Removing Certain Ad Targeting Options and Expanding Our Ad Controls.” META FOR BUSINESS. Accessed March 30, 2023. <https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls>.

BIBLIOGRAPHY

- “RescueTime: Fully Automated Time Tracking Software.” RESCUETIME. Accessed April 1, 2023. <https://www.rescuetime.com/>.
- “Roach Motel.” WIKIPEDIA. Accessed November 2, 2023. [https://en.wikipedia.org/w/index.php?title=Roach Motel](https://en.wikipedia.org/w/index.php?title=Roach_Motel).
- “Share of Ad-Selling Companies in Digital Advertising Revenue in the United States from 2020 to 2025.” STATISTA. (May 2023). <https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/> (accessed November 2, 2023).
- “Snake Charming.” WIKIPEDIA. Accessed November 2, 2023. [https://en.wikipedia.org/w/index.php?title=Snake charming](https://en.wikipedia.org/w/index.php?title=Snake_charming).
- “Supply and Demand.” BRITANNICA. Accessed March 1, 2023. <https://www.britannica.com/topic/supply-and-demand>.
- “Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights.” AMNESTY INTERNATIONAL. (November 21, 2019). <https://www.amnesty.org/en/documents/pol30/1404/2019/en/> (accessed November 2, 2023).
- “TCF 2.2 Launches! All You Need To Know.” IAB.EUROPE. (May 16, 2023). <https://iabeuropa.eu/all-news/tcf-2-2-launches-all-you-need-to-know/> (accessed November 2, 2023).
- “Temporarily Deactivate Your Facebook Account.” FACEBOOK HELP CENTER. Accessed February 22, 2023. https://www.facebook.com/help/214376678584711?helpref=faq_content.
- “Terms and Conditions of Use.” SPOTIFY. Accessed February 23, 2023. <https://www.spotify.com/uk/legal/end-user-agreement/>.
- “Terms of Service.” FACEBOOK. Accessed November 15, 2022. <https://www.facebook.com/terms.php>.
- “The Biggest Companies in the World in 2021.” VISUAL CAPITALIST. Accessed October 10, 2022. <https://ourworldindata.org/explorers/population-and-demography>.
- “The Cost of Ad Blocking.” DARKPONY DIGITAL. Accessed March 30, 2023. <https://www.darkpony.com/blog-en/the-cost-of-ad-blocking/>.
- “The Digital Services Act Package.” EUROPEAN COMMISSION. (April 25, 2023). <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (accessed November 2, 2023).
- “The Economic Value of Behavioral Targeting in Digital Advertising.” IHS MARKIT. (2017). https://datadrivenadvertising.eu/wp-content/uploads/2017/09/BehaviouralTargeting_FINAL.pdf (accessed November 2, 2023).
- “The Illegal Pet Trade: Game Over.” EUROGROUP FOR ANIMALS. (June 1, 2020). <https://www.eurogroupforanimals.org/library/illegal-pet-trade-game-over> (accessed November 2, 2023).
- “The Power of Emotion Analytics.” THINK WITH GOOGLE. Accessed March 7, 2023. <https://www.thinkwithgoogle.com/intl/en-154/marketing-strategies/data-and-measurement/emotion-analytics-powerful-tool-augment-gut-instinct/>.
- “The Power of Emotional Targeting in Advertising.” THEVIEWPOINT. (July 6, 2021). <https://theviewpoint.com/insights/the-power-of-emotional-targeting-in-advertising> (accessed November 2, 2023).
- “The Privacy Sandbox: Technology for a More Private Web.” GOOGLE PRIVACY SANBOX. Accessed April 23, 2023. <https://privacysandbox.com/>.
- “The Value of Digital Advertising.” IAB EUROPE. Accessed January 16, 2023. <https://iabeuropa.eu/the-value-of-digital-advertising/>.

BIBLIOGRAPHY

- “Topics API Overview.” 2022. CHROME FOR DEVELOPERS. Accessed January 25, 2022. <https://developer.chrome.com/docs/privacy-sandbox/topics/overview/>.
- “Tracking-Free Ads Coalition.” TRACKING-FREE ADS COALITION. Accessed May 5, 2023. <https://trackingfreeads.eu/>.
- “VPN Cost?” 2022. NORDVPN. Accessed June 10, 2022. <https://nordvpn.com/pricing/>.
- “Vulnerability and Flourishing – Martha Nussbaum.” HIGHBROW. (October 26, 2017). <https://gohighbrow.com/vulnerability-and-flourishing-martha-nussbaum/> (accessed November 2, 2023).
- “Web Beacon.” NAI: NETWORK ADVERTISING INITIATIVE. Accessed January 4, 2023. <https://thenai.org/glossary/web-beacon/>.
- “Where Did All the ‘Reject’ Buttons Come From?!” NOYB. Accessed October 27, 2023. <https://noyb.eu/en/where-did-all-reject-buttons-come>.
- “World Wide Web.” WIKIPEDIA. Accessed November 2, 2023 https://en.wikipedia.org/w/index.php?title=World_Wide_Web.
- “Young Kids and YouTube: How Ads, Toys, and Games Dominate Viewing.” COMMON SENSE, AND C.S. MOTT CHILDREN’S HOSPITAL (MICHIGAN MEDICINE). Accessed November 2, 2023. https://www.common sense media.org/sites/default/files/research/report/2020_young_kidsyoutube-report_final-release_forweb_1.pdf.
- “YourAdChoices.” YOURADCHOICES. Accessed March 1, 2023. <https://youradchoices.com/about>.

Audiovisual Recourses

- Belfast Buddhist* (2016). “Alan Watts – Choice.” YOUTUBE. Accessed November 2, 2023. <https://www.youtube.com/watch?v=wyUJ5l3hyTo>.
- Chicago Symphony Orchestra* (2015). Beethoven 9 – Chicago Symphony Orchestra – Riccardo Muti, YOUTUBE. Accessed November 2, 2023. <https://www.youtube.com/watch?v=rOjHhS5MtvA>
- Coppola, Francis Ford (1972). *The Godfather*. Paramount Pictures.
- CPDP Conferences* (2023) “The End of Online Behavioral Advertising.” YOUTUBE. Accessed November 2, 2023. <https://www.youtube.com/watch?v=FwMz7OLoOXI>.
- Ewafa* (2017). “Sean Parker - Facebook Exploits Human Vulnerability (We Are Dopamine Addicts)”. YOUTUBE. Accessed November 2, 2023. <https://www.youtube.com/watch?v=R7jar4KgKxs>.
- Kubrick, Stanley (1971). *A Clockwork Orange*. Warner Bros. Pictures.
- Lex Zard* (2021). “Online Targeted Advertising and Human Dignity: Prof. Floridi, Prof. Frischmann, Prof. Zuboff.” YOUTUBE. Accessed November 2, 2023. <https://www.youtube.com/watch?v=WwXG4ZiKw6s>.
- Nolan, Christopher (2008). *The Dark Knight*. Warner Bros. Pictures.
- Nolan, Christopher (2010). *Inception*. Warner Bros. Pictures
- Taylor, Alan (2007) *Mad Men: Smoke Gets Into Your Eyes*. Weiner Bros. Productions.
- The Wachowskis (1999). *The Matrix*. Warner Bros. Pictures
- Weir, Peter (1990). *Dead Poet Society*. Buena Vista Pictures Distribution.

GLOSSARY

GLOSSARY

AdTech	broadly understood “AdTech” refers to advertising technology, including all technical tools for online advertising. This thesis refers to AdTech with its narrow meaning, often used within the policy to describe the industry and supply chain of open advertising exchange (“open exchange”).
Ad Exchange	ad intermediary that provides a sales channel and a technology platform that facilitates programmatic real-time auction in the open exchange of online advertising.
Ad Intermediary	digital service providers that intermediate online advertising, including ad networks, ad exchanges, Demand Side Platforms (DSP), Supply Side Platforms (SSPs), Data Management Platforms (DMPs), and Consent Management Platforms (CMPs).
Ad Network	ad intermediary provides publishers with outsourced sales ability, and advertisers aggregate advertising spaces from numerous publishers.
Advertiser	a legal or natural person paying for the advertisement.
Alphabet	<i>Alphabet Inc.</i> provides the following core platform services: Google Search, YouTube, Google Maps, Google Shopping, and Google Play, including ad intermediaries Google Ads (ad server), AdSense (ad network), Google Display Network (ad network), DV360 (DSP), Google AdX (ad exchange), DFP (SSP).
Capability Approach	a theoretical framework that focuses on the actual capability of persons to achieve lives they value instead of focusing on having a right or freedom to do so.
Core Platform Service	“platforms” listed in Article 2(2) Digital Markets Act (DMA), including online search engines.
Data Management Platforms	ad intermediaries that enrich vendors with consumer data. DMPs sometimes also provide

GLOSSARY

	algorithmic tools for OBA optimization and targeting.
Demand Side Platform	ad intermediary that provides advertisers with the capability to buy aggregated advertising spaces from numerous ad intermediaries and publishers
Digital Services	“information society services” with the meaning of Article 3(a)DSA
Gatekeepers	core platform service providers are designated as “gatekeepers” according to Article (3) DMA.
Harms	legally relevant adverse effects.
Human dignity	a legal concept that recognizes human beings as the source and the boundary of political and economic power. EU case-law has used the concept to recognize and protect the minimum quality of life that all human beings are entitled to live.
Meta	<i>Meta Inc.</i> provides the following core platform services: Facebook, Instagram, WhatsApp, including Meta Audience Network (ad network).
Non-platform Publisher	publishers that do not provide platform services.
Online Platform	platform service as within the meaning of Article 3 (i) Digital Services Act (DSA): “that at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service.” Such a definition covers platform services that provide social media, including social networks and video-sharing platform services.
Online Search Engine	platform service as defined by Article 3 (j) DSA: “that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.”

GLOSSARY

Open Exchange	an open market for online advertising where advertising spaces are traded over ad exchanges. Open exchange is sometimes referred to as “AdTech”.
Platform	digital service that provides intermediation. Defined as “intermediation service” by the Article 3(g) DSA. Platform services include “online platform” and “online search engine” services as defined by the DSA.
Publisher	digital service provider that publishes advertising on their online interface, including platform providers and non-platform publishers.
Supply Side Platform	ad intermediary that provides publishers with outsourced sales ability.
Vendor	digital service provider that engages in online advertising as a publisher, advertiser, or advertising intermediary.
Walled Garden	ad networks provided by the platform service providers, such as Alphabet and Meta, are closed ecosystems that provide complete end-to-end technical solutions for advertisers and publishers.

SAMENVATTING (DUTCH SUMMARY)

MACHT EN WAARDIGHEID: het einde van online gedragsreclame in de EU

Online Behavioral Advertising (OBA) is een online fenomeen dat consumenten gepersonaliseerde advertenties toont op basis van hun gedragsgegevens. OBA is één van de verschillende configuraties van online adverteren – het is een vorm van gepersonaliseerde reclame waarbij een individuele consument wordt benaderd en gesorteerd in segmenten op basis van interesses (“surfliefhebber”) of gedetailleerde demografische kenmerken (“top 10% huishoudinkomen”) die kunstmatige intelligentiesystemen (AI) afleiden op basis van gedragsgegevens over de consument. De gedragsgegevens waarop het algoritme zich baseert voor het afleiden van de consumenteninteresses en -eigenschappen kunnen onder andere het surfen op het internet (bijv. bezochte websites, gebruikte apps) of gedrag op sociale media (bijv. klikken, vind-ik-leuks, bezoeken), muiscursorbewegingen, locatie of toetsenbordaanslagen omvatten.

Grote digitale platformaanbieders, met name Alphabet en Meta, zijn de meest prominente OBA-uitgevers, waardoor adverteerders niet alleen op hun platforms (bijv. YouTube, Instagram) kunnen adverteren, maar ook op websites en apps van andere digitale dienstverleners (bijv. online kranten) die zich bij hun netwerken aansluiten (bijv. Google Display Network, Meta Audience Network). Deze advertentienetwerken zijn gesloten ecosystemen waar platformaanbieders end-to-end controle hebben over OBA-verkoop en worden ‘walled gardens’ genoemd. Alphabet domineert de markt voor zoekadvertenties en Meta domineert de advertentiemarkt voor sociale media. Daarnaast domineert Alphabet de open uitwisselingsmarkt voor OBA, ook wel AdTech genoemd, waar alle advertentienetwerken, uitgevers en adverteerders bieden op advertentieruimte. OBA levert de belangrijkste bijdrage aan de inkomsten van Alphabet en Meta.

Voor de uitvoering van OBA zijn een complexe infrastructuur en technologische capaciteiten vereist, waaronder AI-systemen die consumentenkenmerken afleiden, ‘kwaliteitsscores’ voor advertenties meten en deze aan consumenten toewijzen. Een essentieel onderdeel van deze infrastructuur en processen zijn consumentengegevens. Het verzamelen van consumentengegevens voor OBA vereist het traceren van consumenten via internet, wat doorgaans gebeurt door het plaatsen van zogenaamde “cookies” op consumentenapparaten. Digitale dienstverleners concurreren met elkaar in walled gardens of op de AdTech open beurs. Dit gebeurt voornamelijk via programmatische (volledig geautomatiseerde) veilingen in real-time bidding (RTB). De RTB-veiling wordt doorgaans gewonnen door de partij die de meeste gegevens over de consument bezit, hetgeen leidt tot concurrentie op het extraheren van consumentengegevens. Aangezien grote platformaanbieders zoals Alphabet en Meta de toegang tot consumentengegevens controleren, domineren zij de OBA-markten.

Omdat consumentengegevens essentieel zijn voor OBA, worden leveranciers van digitale diensten gestimuleerd om zoveel mogelijk gegevens over de consument te verzamelen. OBA wordt doorgaans geoptimaliseerd om ervoor te zorgen dat de kans dat consumenten actie ondernemen op advertenties zo groot mogelijk is. In beide gevallen zijn aanbieders van digitale diensten in staat om consumenten op verborgen wijze te beïnvloeden om meer gegevens te verstrekken en op specifieke advertenties te reageren. Dit proefschrift verwijst naar consumentenmanipulatie via OBA als gevallen waarin aanbieders van digitale diensten consumenten manipuleren om OBA mogelijk te maken (manipulatieve extractie) of OBA gebruiken op een manier die leidt tot consumentenmanipulatie (manipulatieve advertentiepersonalisatie).

Manipulatie kan worden gedefinieerd als de succesvolle en opzettelijke poging van een actor om een doelwit te beïnvloeden in de richting van een vooraf bepaald resultaat, waarbij het doelwit zich niet bewust is van een essentieel aspect van de beïnvloeding en de actor zich ervan bewust is dat de beïnvloedingsmethode de kwetsbaarheid van het vermogen van het doelwit om besluiten te vormen waarschijnlijk zal uitbuiten. Consumentenmanipulatie via OBA verwijst naar de situaties waarin aanbieders van digitale diensten consumenten beïnvloeden om hun gegevens (en hun aandacht en tijd) weg te geven of om op een advertentie in te gaan, terwijl de consument zich niet bewust is van een essentieel aspect van deze invloed, terwijl de aanbieder van de digitale dienst zich er tegelijkertijd van bewust is dat deze invloed de kwetsbaarheden in de besluitvorming van de consument kan uitbuiten. Aanbieders van digitale diensten oefenen een manipulatieve invloed uit wanneer zij zich doelbewust richten op het uitbuiten van de kwetsbaarheden van consumenten of wanneer zij er geen rekening mee houden dat hun OBA-praktijken (met inbegrip van ingezette AI-systemen) waarschijnlijk de kwetsbaarheden van consumenten zullen uitbuiten.

Consumentenmanipulatie via OBA vindt plaats wanneer aanbieders van digitale diensten online interfaces ontwerpen met standaardfuncties (bijvoorbeeld automatisch afspelen, personaliseren van content, eindeloze feeds, gamificatie) die de hoeveelheid geëxtraheerde gegevens van de consument maximaliseren zonder alternatieven en betekenisvolle transparantie over de economische logica en risico's die daarmee gepaard gaan. De meest voorkomende manipulatieve praktijken van OBA zijn strategieën die aanbieders van digitale diensten gebruiken om toestemming van consumenten te verkrijgen om hun gegevens weg te geven: aangezien de EU wetgeving OBA alleen toestaat als consumenten toestemming geven, gebruiken aanbieders van digitale diensten een verscheidenheid aan manipulatieve (en dwingende) praktijken om consumenten te beïnvloeden om “toestemming” te geven voor gegevensverwerking.

De OBA-industrie gaat steeds meer over van tracking door derden naar ‘lokale’ of browsergebaseerde advertentiemethoden die het aantal keren dat consumenten toestemming geven voor OBA aanzienlijk zullen verminderen. Dergelijke gecentraliseerde toestemming kan ook worden gemanipuleerd en consumenten

blootstellen aan verdere manipulatie door gepersonaliseerde advertenties. Consumentenmanipulatie via OBA vindt plaats bij het personaliseren van advertenties door essentiële informatie te verbergen of niet vrij te geven (bijvoorbeeld criteria van adverteerders), maar ook door het gebruik van targetingcriteria (bijvoorbeeld het benaderen van onlangs gescheiden mensen) die kwetsbaarheden van consumenten kunnen uitbuiten. Consumentenmanipulatie kan ook plaatsvinden wanneer aanbieders van digitale diensten geen rekening houden met het feit dat de ingezette algoritmen zich op een consument kunnen richten op een manier die misbruik maakt van zijn kwetsbaarheid (bijvoorbeeld een lookalike publiek).

Consumentenmanipulatie via OBA kan leiden tot een direct economisch verlies voor de consument of tot structurele schade door marktfalen, zoals verminderde innovatie, verminderde kwaliteit van inhoud en diensten, hogere prijzen, verminderde welvaart en een verminderd vertrouwen in de markt. Het kan ook bijdragen aan milieuschade door een toename van de CO₂-uitstoot, overmatig gebruik van batterijen en elektronisch afval, en kan ook een negatief effect hebben op het dierenwelzijn. Het kan leiden tot sociaal-maatschappelijke schade zoals discriminatie en onderdrukking van specifieke (vaak gemarginaliseerde) groepen. De schadelijke gevolgen voor de privacy bestaan onder meer uit emotioneel leed, verstoring, gefrustreerde verwachtingen en angst. Over het algemeen kan manipulatie worden opgevat als ‘tijddiefstal’ die leidt tot schade aan de authenticiteit, zoals verlies van (tijd voor) samenleven, vrije tijd en inkomsten. Consumentenmanipulatie via OBA kan ook leiden tot integriteitsschade, waaronder ernstige nadelige gevolgen voor de geestelijke en lichamelijke gezondheid en welzijn (bijvoorbeeld zelfbeschadiging en verlies van leven). Ten slotte kan consumentenmanipulatie via OBA leiden tot schade aan de waardigheid van toekomstige generaties, democratische processen en het zelfrespect van de consument door het verankeren van systeemrisico's in de onlineomgeving om kwetsbaarheden van consumenten te exploiteren.

In dit proefschrift wordt de vraag gesteld in hoeverre het juridisch kader van de Europese Unie (EU) bescherming biedt tegen de veroorzaakte schade van OBA door consumentenmanipulatie. Het juridisch kader van de EU voor consumentenmanipulatie via OBA omvat drie rechtsgebieden: (1) het consumentenbeschermingsrecht, in het bijzonder de richtlijn betreffende oneerlijke handelspraktijken, de richtlijn betreffende consumentenrechten, en de richtlijn betreffende oneerlijke bedingen in consumentenovereenkomsten; (2) wetgeving inzake gegevensbescherming en privacy, in het bijzonder de algemene verordening gegevensbescherming (AVG) en de richtlijn betreffende privacy en elektronische communicatie; en (3) het mededingingsrecht, gebaseerd op de artikelen 101 en 102 van het Verdrag betreffende de werking van de Europese Unie (VWEU).

Het rechtskader van de EU omvat ook andere wetgeving die is aangenomen binnen de EU-strategie voor een digitale interne markt, met name de richtlijn audiovisuele mediadiensten in het licht van een veranderende marktsituatie, de ter

bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten, de richtlijn betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten, de digitale dienstenverordening (DDV), de digitale marktenverordening (DMV) en initiatieven voor de wet op de kunstmatige intelligentie (WAI).

Dit proefschrift constateert dat het EU-rechtskader bescherming biedt tegen de schade van consumentenmanipulatie via OBA door op vier manieren grenzen te stellen aan consumentenmanipulatie via OBA: (i) door verboden in te voeren voor onwettige OBA-praktijken, zoals het benaderen van minderjarigen of het gebruik van bijzondere categorieën gegevens; (ii) door regels voor openbaarmaking van informatie (bijv. adverteerders, targetingcriteria) in te voeren om transparantie voor consumenten te garanderen; (iii) door regels voor risicobeoordeling en -beperking in te voeren om de verantwoordelijkheid van aanbieders van digitale diensten en de eerlijkheid van hun praktijken te garanderen, en (iv) door regels voor transparantie en gegevenstoegang in te voeren die handhavers in staat stellen aanbieders van digitale diensten ter verantwoording te roepen voor hun OBA-praktijken. Het rechtskader van de EU biedt handhavers stevige mogelijkheden. De Europese Commissie in het bijzonder is sinds de implementatie van de DDV en DMV een 'one-stop-shop' geworden voor Alphabet en Meta, die de belangrijkste begunstigden en bepalers van standaarden in de OBA-industrie zijn, voor het monitoren en afdwingen van de naleving van het EU-rechtskader.

Dit proefschrift concludeert dat het wettelijk kader van de EU beschermt tegen alle schade die OBA veroorzaakt door consumentenmanipulatie. De afzonderlijke onderdelen van het wettelijk kader beschermen direct of indirect tegen schade. Het voornaamste doel van de richtlijn oneerlijke handelspraktijken is bijvoorbeeld om de economische belangen van consumenten te beschermen door ervoor te zorgen dat zij een authentieke keuze kunnen maken. De richtlijn oneerlijke handelspraktijken waarborgt de privacy van consumenten op indirecte wijze wanneer dit essentieel is voor de bescherming van de economische belangen van consumenten. Als gevolg van het garanderen van authentieke keuze beschermt de richtlijn oneerlijke handelspraktijken ook tegen andere schade die gepaard gaat met economische schade. De AVG, de DDV en de DMV vullen de richtlijn betreffende oneerlijke handelspraktijken aan om samen een solide raamwerk te bieden om grenzen te stellen aan consumentenmanipulatie via OBA. Dit kader biedt zowel inhoudelijke regels als handhavingsmodelijkheden die nodig en toereikend zijn om te beschermen tegen de schade van consumentenmanipulatie door OBA. Derhalve zal het in stand houden van wettelijke grenzen grotendeels afhangen van de handhavingsactie.

CURRICULUM VITAE

Aleksandre Zardiashvili (*alias* Lex Zard),¹⁴⁵⁷ was born in Tbilisi, Georgia, in 1992. In 2014, he graduated with a Bachelor of Laws (LL.B) from Caucasus University. After a short experiment with managing an e-commerce start-up in 2014-2015, he started working at the anti-money laundering supervision department of the National Bank of Georgia (NBG). Lex was responsible for off-site monitoring of financial institutions and their on-site inspections. In 2015-2017, Lex led highly consequential on-site inspections in large commercial banks. During this time, Lex became interested in digital transformation governance. In 2017 he joined Advanced Master's Program in *Law and Digital Technologies (LDT)* at Leiden University, where he graduated *cum laude*.

In 2018, Lex joined eLaw – *Center for Law and Digital Technologies* at Leiden University as a researcher and teacher focused on responsible artificial intelligence (AI). In 2019, Lex won the EURA Young Scholar Prize. In 2019, he started working on his Ph.D. research regarding online behavioral advertising (OBA), resulting in this thesis. In 2019-2022, Lex helped coordinate the Advanced Master's Program LDT, organized various events, and gave lectures in multiple courses. Lex coordinated a *Digital Technologies & Power* class within the *Responsible Innovation* minor program. In July 2023, Lex participated in the Oxford Internet Institute Summer Doctoral Program.

List of publications:

Lex Zard, *Five Years of Illegitimacy of Surveillance Advertising*, in CRITICAL REFLECTIONS ON THE EU'S DATA PROTECTION REGIME: GDPR IN THE MACHINE (Róisín Costello & Mark Leiser, eds.) (forthcoming 2024).

Lex Zard, *Consumer Manipulation via Online Behavioral Advertising*, B.U.J. SCI. & TECH. L. 30 (2), (forthcoming, 2024).

Andreas Häuselmann, Alan M. Sears, **Lex Zard** & Eduard Fosch-Villaronga, *European Union Law of Emotion Data*, Conference paper for 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII) (2023).

Lex Zard & Alan M. Sears, *Targeted Advertising and Consumer Protection Law in the European Union*, VAND. J. TRANSNAT'L L. 56(3): 799-852 (2023).

¹⁴⁵⁷ Lex has previously published as Lexo Zardiashvili.

Lexo Zardiashvili & Eduard Fosch-Villaronga, “*Oh, Dignity, too?*” *Said the Robot: Human Dignity as the Basis for the Governance of Robotics*, 30 MINDS & MACH. (1): 121-143 (2020).

Lexo Zardiashvili & Eduard Fosch-Villaronga, *Artificial Intelligence in Healthcare through the Lens of Human Dignity*, in LEGAL, SOCIAL AND ETHICAL PERSPECTIVES ON HEALTH & TECHNOLOGY (Fathisalout-Bollon & Anna Berti Suman, eds.) 45-64 (2020).

Lexo Zardiashvili, Jordi Bieger, Francien Dechesne, & Virginia Dignum, *Artificial Intelligence Ethics for Law Enforcement: A Study into Requirements for Responsible Use of AI at the Dutch Police*, 2(4) DELPHI – INTERDISC. REV. EMERGING TECH. (2019).

Francien Dechesne, Virginia Dignum, **Lexo Zardiashvili** & Jordi Bieger, *Long-term Research Strategy for Artificial Intelligence and Ethics at the Police*, AIEP, 2019.

Francien Dechesne, Virginia Dignum, **Lexo Zardiashvili**, & Jordi Bieger, *AI and Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police*, AIEP, 2019.

Lexo Zardiashvili & Francien Dechesne, *Consumer Control of Energy Data: The Need for the Consent Management Mechanism in the Energy Sector of the Netherlands and Roadblocks Related to its Implementation*, SCALES, 2019.

Mark R. Leiser, **Lexo Zardiashvili** & Francien Dechesne, *Realizing the Full Potential of the Right to Data Portability: Using Data Protection for Healthcare Innovation*, SCALES, 2019.

INDEX

- Article 29 Working Party (A29WP), 156, 175, 177-178, 212, 225.
- access-for-data bargain, 81.
- ad exchanges, 4, 33, 268, 270.
- ad networks, 4, 27, 28-30, 190, 204, 268, 270.
- ad servers, 30, 157, 204.
- ad-blockers, 126, 136, 259.
- addictive design, 87, 210.
- AdTech, 4, 27-34, 157-159, 189-190, 194-195, 203, 206, 213, 218, 223-226, 270-271.
- artificial intelligence (AI) 5, 7, 23, 42, 61, 75, 83, 93, 97, 103, 120, 161, 167, 168, 170, 174, 185-188, 205, 212-219, 226-227, 235, 243-244, 255-258, 271-276.
- Alphabet, 1-6, 21-41, 107, 126-132, 152, 156, 158-159, 163-165, 169-173, 190, 194, 196, 202-224, 262-271, 274
- animal welfare, 122, 131-132, 143, 220
- attention (consumer), 2, 4, 14, 54, 69, 79, 80, 83-93, 100, 103, 117, 128, 131, 139-140, 150, 185, 202, 205, 210, 219, 227.
attention economy, 84.
- automated behavior patterns, 54.
- autonomy, 5, 9, 11, 13, 62, 108-134, 143, 146-149, 154, 158, 161, 187, 189, 209, 213, 229
- auto-play, 86-87, 103, 137, 219
- average consumer, 53, 74, 147, 149, 151, 180, 183, 184
- Audiovisual Media Services Directive (AVMSD), 162, 221.
- behaviorism, 17-18, 71.
- bias (cognitive), 14, 53-62, 74, 109.
- bioethics, 60.
- bounded rationality, 74, 77, 151.
- Cambridge Analytica, 13, 77, 207-208.
- capability approach, 121-122, 142.
- competition authorities (CAs), 157, 207.
- Charter of Fundamental Rights of the European Union (CFREU), 6, 9, 88, 114, 115, 117, 118-140, 152, 188, 209.
- Court of Justice of the European Union (CJEU) 10, 74, 88, 107, 138, 151, 157, 160, 171-172, 178, 182, 184, 192-195, 200, 203, 213, 215, 226, 228, 233, 239, 259, 260.
- click-wrap contracts, 82.
- consent management platform (CMP), 89, 194, 268.
- coercion, 8, 14, 44-49, 55, 60, 67, 68, 104, 179, 181, 187, 197.
- Compass Banca (CJEU)*, 74, 151, 184, 233.
- competition (market, law), 6, 7, 9, 11, 15, 29, 31, 42, 111-113, 122, 129-130, 145-146, 156-163, 169, 213, 216-224, 228, 239.
- consent, 34, 60, 88-92, 115, 117, 141, 148, 152-155, 160, 166, 177, 179, 180, 181, 188, 189, 190, 191, 192, 193, 194, 195, 196-203, 210, 211, 213, 215, 217, 219, 223-225, 252, 258, 262, 265.
- constitutionalism, 108, 114, 115, 120, 138.
- consumer manipulation market trap, 126, 128, 129, 130, 160.
- consumer welfare, 109-113, 125-130, 156, 161, 227-228.
- content moderation, 164.
- contextual advertising, 22, 32.
- cookies, 11, 33-41, 88-92, 125, 153, 154, 190, 194-195, 211, 218, 257, 259, 261, 271.
cookie banners, 80, 88-92, 127, 145, 153, 154, 194.
- core platform services, 164-165, 268, 269.
- consumer protection authorities (CPAs), 33, 151, 207.
- dark patterns, 78- 90, 102, 107, 117, 181.
- Digital Content Directive (DCD), 162, 185, 196, 197, 198, 214, 220, 221
- deception, 52, 56
- democracy, 5, 6, 13, 114, 119, 139, 143-144, 201, 211.
- discrimination, 5, 13, 24, 118, 122, 124, 132, 133, 143, 144, 146, 161, 172, 178, 209, 220
- Digital Marketers Act (DMA), 4, 7, 10, 163-167, 190-193, 203, 209-211, 214-216, 220-225, 237, 243, 247, 268, 269
- data management platforms (DMPs), 29, 35, 268-269.
- DoubleClick, 31, 157-158, 159, 234, 247, 263.
- data protection authority (DPA), 176, 190, 192-195, 199-203, 254, 261.
- data protection impact assessment (DPIA), 155, 212, 213, 226, 235.
- Digital Services Act (DSA), 7, 10, 161-183, 203-226, 236, 247, 257, 260, 269-270.
- demand side platform (DSP), 28, 29, 31, 33, 35, 159, 204, 268.

- European Data Protection Board (EDPB), 10, 155, 199-201, 206-209, 223-225, 237.
- efficiency
advertising efficiency 16, 20, 29, 71.
market efficiency, 110, 113, 156, 228, 229.
- endless feed, 86-87, 103, 219.
- engagement (consumer), 25, 81, 86-87, 140
- environmental (harms, interests), 13, 15, 63, 118, 122, 130, 143, 184, 211, 219.
- ePrivacy Directive, 6, 88, 153, 194, 214, 220
- European Commission, 5-7, 13, 21-24, 27-28, 30-32, 38, 41, 45, 54, 61, 74-75, 78, 80, 82, 85, 86, 90, 92, 96, 100-116, 120, 125, 127, 128, 130, 134, 136, 145, 152, 156-159, 163-167, 169-170, 172, 174, 183, 185, 202, 205-209, 216-227, 234-237, 263, 266.
- extended reality (xR), 78, 226.
- fairness, 120, 125, 154, 161-167, 212-214, 220, 227, 229.
- filter bubble, 85.
- fingerprinting (device), 40.
- gatekeepers, 2, 7, 27, 29, 32, 84, 92, 126, 128-129, 160, 165-167, 190-196, 202-203, 209-210, 213-215, 222-226, 269.
- General Data Protection Regulation (GDPR), 6, 9, 32, 89, 102, 127, 152-156, 165, 170-203, 210-215, 220-227, 237, 248, 250, 254-255, 257, 262, 265, 275
- Godfather* (the), 47, 66, 267.
- harms, 6-16, 43, 45, 69, 105-152, 160-175, 182-190, 205, 207, 209, 210, 211, 213, 215, 216, 217, 220, 221, 222, 224, 226
- heuristics, 54.
- human condition, 60, 63.
- human dignity, 6, 114-123, 134, 138, 140, 141-143, 209, 227.
- humanity formula (Kant), 106, 114, 138.
- Interactive Advertising Bureau (IAB), 30, 92, 194-195, 203, 238, 249, 264, 266.
- information age, 107-109, 138.
- information paradigm, 147.
- intermediation, 26-28, 42, 130, 157, 158, 162, 163, 164, 204, 270.
- inventory, 26, 29, 30, 33.
- layers (of vulnerability), 65, 68, 183.
- legibility, 27.
- liberalism, 107-108, 113, 120.
- lookalike audiences, 24.
- manipulation, 5-16, 41-70, 73-96, 101, 103, 105-151, 160-170, 172, 174, 175, 179-188, 197, 203, 205, 208-226, 250, 258.
manipulation-as-a-service, 89.
 online manipulation, 11, 75, 79.
 digital market manipulation, 11, 74, 75.
 manipulative extraction practices, 81, 83, 104, 130, 181.
 market failure, 72, 111, 136.
 market-based (interests, harms), 109, 136.
 martini, 56, 66-67.
- Meta, 1-7, 23-27, 30-38, 40, 42, 49, 78, 83, 89, 107, 126-129, 156, 159-160, 165-166, 169, 171, 173, 176-177, 182, 190, 192-193, 198-208, 212, 218, 222-228, 233, 236-237, 242, 257, 259-265, 269-271, 274.
- Meta v. Bundeskartellamt*, 160, 166, 192, 193, 200, 202, 203, 215, 228.
- nudges, 57, 58, 91.
- online behavioral advertising (OBA), 8, 11, 16, 24, 25, 32, 41, 43, 69, 105, 217, 275.
- OBA contracts, 185, 196, 197, 198, 225
- OBA-or-Pay, 92, 191, 192, 193, 196, 224, 225, 226.
- Omega Judgment*, 138.
- online platforms (DSA), 1, 21, 107, 128, 163, 164, 165, 166, 170, 171, 172, 173, 174, 175, 176, 180, 181, 204, 205, 206, 212, 214, 215, 224, 225
- OpenRTB (protocol) 34, 194, 265.
- Orange Polska (CJEU)*, 182, 233
- Platform-to-Business Regulation (P2BR), 162, 214, 220, 221
- personal data, 6, 22-23, 41, 88, 116-118, 122, 125, 134-135, 146, 148, 151-156, 160-166, 168, 170-177, 185, 188-189, 194, 196-202, 209-212, 219, 223-226, 237.
- personalized pricing, 24.
- personalizing, 24, 69, 80, 88, 96-97, 100.
- Persuasion Knowledge Model (PKM), 73, 244.
- preferences, 14, 23, 36, 53, 56, 57, 71, 72, 76, 80, 89, 108, 110, 123, 128, 147, 170, 184, 194, 201, 205, 215
- Privacy Enhancing Technologies (PETs), 211
- Privacy Sandbox, 39, 41, 154, 196, 257, 263, 266.
- professional diligence, 149-150, 174, 182, 213
- profiling (behavioral personalization), 13, 23-25, 100, 175, 177, 235, 243, 246, 249, 255.
- programmatically auction, 14, 16, 33.
- psychological profiling, 98-99.
- quality of life, 108, 115-118, 120-121, 137, 227, 228, 269.
- rationality, 53.

INDEX

- Real-Time Bidding (RTB), 4, 33-34, 194, 254, 262, 265.
- recommender systems, 24, 85, 168, 205, 208, 209, 210, 212.
- repositories (advertising), 173, 175, 206-208, 209, 226.
- re-targeting, 25.
- Rhine capitalism, 112.
- rights-based (harms, interests), 14, 105, 108, 109, 113-114, 118-122, 136.
- scattered damage, 124.
- Schufa* (CJEU), 178, 233
- seduction, 44, 56, 67.
- sniper ad targeting, 101-104.
- special categories, (of data) 155, 165, 170-175, 214, 224.
- supply side platform (SSP), 29-30, 33, 38, 164, 268.
- subliminal (techniques, advertising), 49, 50, 72, 162, 168, 185, 186.
- tags, 37, 38, 153.
- Transparency Consent Framework (TCF), 92, 194-196, 203, 249, 257, 263, 264, 266.
- Uber ADM Case, 178.
- Unfair Commercial Practices Directive (UCPD), 5, 147-151, 170, 174-175, 179, 186, 206, 211-215, 220-221, 225.
- undue influence, 149, 150, 181.
- unfairness paradigm, 147-148
- vulnerability, 5, 11, 14, 43, 51-52, 55, 59-60, 61-68, 77-78, 84, 87, 94, 99-104, 139, 141-144, 151, 168, 173, 179, 181-184, 187-192, 197, 210, 218-219, 229, 267.
digital vulnerability, 78, 184.
- walled gardens, 28-31, 42, 218, 271.