Targeted advertising and consumer protection law in the European Union

Zardiashvili, A.; Sears, A.M.

Targeted Advertising and Consumer Protection Law in the European Union

Lex Zard* & Alan M. Sears**

ABSTRACT

Targeted advertising is the primary revenue stream for the largest online platforms that act as the internet's gatekeepers, such as Alphabet and Meta. The financial incentives drive targeted advertising towards maximizing the efficiency of algorithmically matching advertisements with consumers, which typically requires building fine-grained profiles that rely on consumers' personal data. In the European Union (EU), the protection of personal data is a fundamental right operationalized by the General Data Protection Regulation (GDPR), establishing the limits of targeted advertising to the extent that it relies on the processing of personal data. Nevertheless, as online interface design and fine-grained personalization allow platforms and other publishers new ways to influence consumers, targeted advertising is also associated with the potential for consumer manipulation.

While the consumer protection framework in the EU is the primary field that protects consumers from manipulation, it has received little attention in academia in the context of targeted advertising when compared with the GDPR. In 2022, the EU adopted proposals for the Digital Services Act (DSA) and the Digital Markets Act (DMA), which contain consumer protection rules that directly limit targeted advertising. These developments in consumer protection law may fundamentally transform the internet, as its gatekeepers are now faced with a new legal regime that regulates their primary source of revenue. This Article provides an overview of the myriad of legislation that comprises the EU consumer protection framework—including how it intersects with the data protection framework—and analyzes how and the extent to which it coalesces to limit targeted advertising.

---

* Researcher and Lecturer at eLaw, Center for Law and Digital Technologies, Faculty of Law, Leiden University, The Netherlands. LL.M., Leiden Law School (2018); B.A., Caucasus Law School (2010). Contact: a.zardiashvili@law.leidenuniv.nl

** Researcher and Lecturer at eLaw, Center for Law and Digital Technologies, Faculty of Law, Leiden University, The Netherlands. LL.M., Leiden Law School (2017); J.D., Notre Dame Law School (2014); B.A., Baylor University (2006). Contact: a.m.sears@law.leidenuniv.nl

Authors would like to thank Egelyn Braun and Bart Custers for their feedback on earlier drafts of this paper, as well as the editors of VJTL for their dedication and hardwork.

TABLE OF CONTENTS

I. INTRODUCTION

One of the key characteristics of the twenty-first century is the rise of online platforms. Some of these platforms act as gatekeepers of the internet that leverage their access to user data and attention and are able to enclose consumers, business customers, and competitors in relational dependency.[1] Such online platforms[2] include marketplaces,[3] search engines,[4] social networks,[5] app stores,[6] and on-demand media streaming services.[7] Companies such as Alphabet[8] and Amazon.com were nearly bankrupt in the early 2000s, and Meta platforms did not

1. *See* Elettra Bietti, *A Genealogy of Digital Platform Regulation*, 7 GEO. L. TECH. REV. 1, 1 (2023).

2. This article refers to "online platforms" to describe providers of digital services that "serve at least two different sets of users simultaneously, bringing them together and enabling interactions between them." 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 [https://perma.cc/PTN5-HZK9] (archived Feb. 26, 2023).

3. For example, Amazon and eBay.

4. For example, Google Search, Google Maps, and Microsoft Bing.

5. For example, Facebook, Instagram, Twitter, and TikTok.

6. For example, the Apple App Store, Google Play, and the Microsoft Store.

7. This includes video-on-demand services such as YouTube, and music-on-demand services such as Apple Music, Spotify, Tidal, Amazon Music Unlimited, and YouTube Music.

8. The technology conglomerate Alphabet, Inc. [hereinafter Alphabet] was formerly known and listed on the stock market as Google, Inc. Google LLC is one of the wholly-owned subsidiaries of Alphabet and it operates, among other things, Google Search, YouTube, Google Chrome, Android, Google Play, and Google Maps. *See G is for Google*, ALPHABET, https://abc.xyz/ (last visited Aug. 12, 2022) [https://perma.cc/43WX-BK5N] (archived Feb. 3, 2023).

exist;[9] together, they exceeded $4 trillion in market capitalization in 2022.[10] These three companies joined Apple and Microsoft Corporation on the list of the most profitable companies in the world, which are now commonly known as Big Tech."[11]

This rise is not surprising, as the users of online platforms place great value on their services.[12] Moreover, internet users often do not directly pay money for these services. Instead, online platforms monetize their services in two different ways. The first way services can be monetized entails charging a commission to retailers (and/or developers) who sell their products, services, or content to users of the platforms.[13] Such primarily *transaction-based* online platforms include, for example, Amazon Store and Apple App Store. The second type of monetization entails charging advertisers who want to promote their products, services, and content to the users of the platform.[14] Such primarily *advertising-based* online platforms include Google Search, YouTube, Facebook, and Instagram. The profitability of these

---

9. Meta, Inc. was formerly known and 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/ [https://perma.cc/WM5A-NUBT] (archived Feb. 3, 2023).

10. Luigi Zinglaes & Filippo Maria Lancieri, *Stigler Committee on Digital Platforms: Policy Brief*, *in* STIGLER COMMITTEE ON DIGITAL PLATFORMS: FINAL REPORT 6, 6 (2019); *see also* LARGEST COMPANIES BY MARKET CAP, https://companiesmarketcap.com/ (last visited Mar. 12, 2023) [https://perma.cc/TZ2R-4ZRB] (archived Feb 3. 2023) (listing Alphabet, Amazon, and Meta as currently each being in the top ten companies with the largest market capitalizations in the world).

11. The 'Big Tech' now usually refers to all five companies together: Alphabet Inc. (owner of Google), Amazon, Apple, Microsoft, and Meta. In 2021, these companies together with Saudi Arabian Oil Company were the largest companies by market capitalization. *See* Jenna Ross, *The Biggest Companies in the World in 2021*, VISUAL CAPITALIST (June 10, 2021), https://www.visualcapitalist.com/the-biggest-companies-in-the-world-in-2021/ [https://perma.cc/374M-BHPH] (archived Feb. 3, 2023). While Alphabet, Amazon, Apple, and Microsoft remain at the very top of the list, Meta has dropped to ninth place. *See* LARGEST COMPANIES BY MARKET CAP, *supra* note 10. Online platforms, excluding Microsoft, are at times classified as 'Big Four' based on their impact on the Internet instead of market capitalization or revenue. *See* Erick Schonfeld, *Eric Schmidt's Gang of Four: Google, Apple, Amazon, and Facebook*, TECHCRUNCH (May 31, 2011, 9:19 PM), https://techcrunch.com/2011/05/31/schmidt-gang-four-google-apple-amazon-facebook/ [https://perma.cc/LPF2-9GUB] (archived Feb. 3, 2023).

12. *See* COMPETITION & MKTS. AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING: MARKET STUDY FINAL REPORT 6 (2020) [hereinafter CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY].

13. *See How to Start Selling on Amazon*, AMAZON, https://sell.amazon.com/sell (last visited Aug. 11, 2022) [https://perma.cc/76BM-TFGT] (archived Feb. 5, 2023); *Apple Media Services Terms and Conditions*, APPLE, https://www.apple.com/legal/internet-services/itunes/us/terms.html (Sept. 12, 2022) [https://perma.cc/2ZSR-H4Y8] (archived Feb. 6, 2023).

14. *See How We Make Money with Advertising*, GOOGLE, https://howwemakemoney.withgoogle.com/ (last visited Feb. 5, 2023) [https://perma.cc/2MWW-HJAQ] (archived Feb. 5, 2023); *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php (last visited Feb. 5, 2023) [https://perma.cc/H9MX-696H] (archived Feb. 5, 2023).

online platforms stems from their position as intermediaries, which enables them to provide their business users and non-business users with *access* to one another, as well as visibility and techniques that render their users *legible* for such matching.[15] Intermediation capabilities of advertising-based online platforms allow their business users to target advertisements to their preferred audience with a high degree of specificity.[16] Consequently, non-business users access online platforms without monetary payment and are exposed to ads that are often personalized.[17]

Google and Meta have expanded their advertising practices outside of their platforms by creating advertising networks (e.g., Google Display Network and Meta Audience Network) that, on the one hand, track users across the internet and, on the other, target them with advertising on a wide variety of websites, including their own. Advertising networks compete in a fully automated auction process that determines the placement of a particular advertisement to target a specific internet user.[18] While Google and Meta operate the most prominent advertising networks and are the primary beneficiaries of targeted advertising, thousands of relatively minor advertising intermediaries have emerged (including those operated by other online platforms, such as Amazon Ads and Apple Search Ads) to create a massive, global targeted advertising ecosystem.[19] This ecosystem enables the functioning of the internet so that non-business users can access the digital services and content of online platforms as well as other publishers (e.g., online newspapers, digital games, etc.) they value without monetary payment.[20]

Nevertheless, targeted advertising has been subject to much controversy within the European Union (EU). While it makes digital services and content accessible to internet users without monetary payment, it is primarily dependent on the processing of the *personal*

---

15. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 137 (2017).

16. *See id.* at 140–43.

17. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 6.

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

19. In 2019, in the U.K., £14 billion was spent on online advertising, 80 percent of which was spent on platforms operated by Google and Meta. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 9; *see also* EU Directorate-General for Internal Policies, Pol'y Dep't for Econ., Sci. & Quality Life Policies, Online Advertising: The Impact of Targeted Advertising on Advertisers, Market Acess and Consumer Choice, PE 662.913, at 24 (2021) [hereinafter EU Pol'y Report Online Advertising];

20. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 6; *see also* EU Pol'y Report Online Advertising, *supra* note 19, at 26–27 ("Depending on the content and the context in which the ad is experienced, the user may view it as potentially valuable, providing useful information . . . [i]n this case, advertisements can help consumers to make purchasing decisions, which better reflect their preferences and are therefore welfare enhancing.").

data of users, which is protected by the fundamental rights framework of the EU.[21] Also, tracking users across the internet is in tension with rules on privacy set out in the Directive on Privacy and Electronic Communications (ePrivacy Directive).[22] In 2016, the EU updated its personal data protection and privacy rules with the landmark General Data Protection Regulation (GDPR)[23] to more effectively safeguard Europeans' privacy and personal data rights with regard to targeted advertising.[24] Moreover, targeted advertising practices have raised issues beyond privacy and data protection, such as consequences of incorrect inferences, consumer manipulation, discrimination, and loss of reputation, as well as issues related to market power, lack of competition, and harm to political processes.[25] The rise of targeted advertising and online platforms came as a significant blow for traditional media, which suffered heavy financial losses.[26]

As the core practices in targeted advertising have remained somewhat unaffected by the GDPR, the EU has taken further steps to tackle the risks of such practices. In response to the potentially negative effects of targeted advertising on elections and political processes, the European Commission (the Commission) proposed the Regulation on Transparency and Targeting of Political Advertising.[27] In response to the lack of competition in the online platform ecosystem, the EU adopted the Digital Markets Act (DMA), introducing new competition law rules for online platforms engaged in targeted

---

21. *See* Charter of Fundamental Rights of the European Union art. 8, Dec. 7, 2000, 2000 O.J. (C 364) 10 [hereinafter CFREU].

22. *See* Directive 2002/58/EC, 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) ¶¶ 24–25 [hereinafter ePrivacy Directive].

23. *See* 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) ¶¶ 6–10 ("Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities . . . Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement.") [hereinafter General Data Protection Regulation].

24. *See* European Commission Press Release IP/10/63, Europeans' Privacy Will be Big Challenge in Next Decade, Says EU Commissioner (Jan. 28, 2010).

25. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 49–51.

26. *See Dutch Publishers Launch Mass Claim against Google over Ads*, DUTCHNEWS.NL (Sept. 13, 2022), https://www.dutchnews.nl/news/2022/09/dutch-publishers-launch-mass-claim-against-google-over-ads/ [https://perma.cc/56UB-4BJT] (archived Feb. 6, 2023); *see also* EU Pol'y Report Online Advertising, *supra* note 19, at 28, 141.

27. *See Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising*, at 1, 3, COM (2021) 731 final (Nov. 25, 2021).

advertising.[28] The Commission has also opened a formal antitrust investigation against Google and Meta.[29] In order to safeguard EU residents from the potentially significant harmful effects of personalization using artificial intelligence (AI) technologies, the Commission has introduced new rules in the Proposal for Artificial Intelligence Act (PAIA).[30] Targeted advertising is also associated with significant risks of discrimination, to which the non-discrimination laws of the EU also apply.[31]

However, targeted advertising is, first and foremost, a market practice directed toward consumers. The economic logic behind the targeted advertising ecosystem creates an incentive for publishers (including online platforms) to create online environments that modify consumer behavior in the interest of maximizing the profit of the ecosystem.[32] Such online environments may exploit consumers' decision-making vulnerabilities and lead them to transactional decisions that may go against their best interests.[33] Such manipulative practices of targeted advertising may erode consumer autonomy and lead to inefficient market outcomes.[34] The EU legal framework for

---

28. *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), 2022 O.J. (L 265) ¶¶ 7–10 [hereinafter Digital Markets Act].

29. *See* European Commission Press Release IP/22/1703, Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google and Meta, in Online Display Advertising (Mar. 11, 2022); *see also* Case T-604/18, Google v. European Commission, ECLI:EU:T:2022:541, ¶ 62 (Sept. 14, 2022) ("Google entered into an agreement with Apple whereby Google Search became the default general search service on all of Apple's smart mobile devices . . . As a result of that agreement Google Search accounted, in 2010, for more than half of the internet traffic on the iPhone and almost a third of all mobile internet traffic.").

30. *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*, at 1, COM (2021) 206 final (Apr. 21, 2021) .

31. *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) (highlighting how, for example, Facebook's "Find the Right Person for Your Business!" targeted advertising strategy has "fostered sex, racial, and age discrimination against users in their access to goods, services, and employment"); Alan M. Sears, *The Limits of Online Price Discrimination in Europe*, 21 COLUM. SCI. & TECH. L. REV. 1, 38–40 (2020).

32. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 200–203 (2019) ("The aim of this undertaking is not to impose behavioral norms, such as conformity or obedience, but rather to produce behavior that reliably, definitively, and certainly leads to desired commercial results.").

33. *See* FRANCISCO LUPIÁÑEZ-VILLANUEVA, ALBA BOLUDA, FRANCESCO BOGLIACINO, GIOVANNI LIVA, LUCIE LECHARDOY & TERESA RODRÍGUEZ DE LAS HERAS BALLELL, BEHAVIOURAL STUDY ON UNFAIR COMMERCIAL PRACTICES IN THE DIGITAL ENVIRONMENT: DARK PATTERNS AND MANIPULATIVE PERSONALISATION 6 (2022) [hereinafter EC STUDY ON DARK PATTERNS AND MANIPULATIVE PERSONALISATION].

34. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1025–26, 1029–30 (2014); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*,

consumer protection is the central area of law that safeguards consumer autonomy in targeted advertising. Nevertheless, consumer protection law has received only limited attention when it comes to regulating targeted advertising.[35]

This Article examines the EU's legal framework on consumer protection to determine the extent to which its provisions safeguard European consumers from potential harms stemming from targeted advertising. In doing so, this Article elaborates on the requirements for publishers of targeted advertising and the limits of targeted advertising imposed by the consumer protection law in the EU.[36] The EU legal framework for consumer protection envisages Unfair Commercial Practices Directive (UCPD),[37] the Consumer Rights Directive (CRD),[38] the Unfair Contract Terms Directive (UCTD),[39] the Digital Content Directive (DCD),[40] and most recently, the Digital Services Act (DSA).[41] Moreover, this Article refers to other EU

---

20 THEORETICAL INQUIRIES LAW 157, 162, 166 (2019); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 38 (2019) ("The hiddenness of manipulation challenges both conditions of autonomy—competency and authenticity. Because manipulees are unaware that features of their choice environments have been intentionally designed to influence them, their capacity to (competently) deliberate is undermined, yielding decisions they cannot endorse (authentically) as their own.").

35. *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) ("So far, personal data have played only a small role in the process of amending the consumer law framework to meet the needs of the digital economy."); Calo, *supra* note 34, at 999; FEDERICO GALLI, ALGORITHMIC MARKETING AND EU LAW ON UNFAIR COMMERCIAL PRACTICES 264–65 (Springer 2022); *see also* JAN TRZASKOWSKI, YOUR PRIVACY IS IMPORTANT TO US! – RESTORING HUMAN DIGNITY IN DATA-DRIVEN MARKETING 181–87 (2021).

36. The laws examined in this article may not be entirely exhaustive; other provisions may exist that have a bearing on the extent to which targeted advertising is legally permitted.

37. Directive 2005/29/EC, of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market 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) arts. 1, 2(d) [hereinafter Unfair Commercial Practices Directive].

38. Directive 2011/83/EU, 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, 2011 O.J. (L 304) [hereinafter Consumer Rights Directive].

39. Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) [hereinafter Unfair Contract Terms Directive].

40. 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, 2019 O.J. (L 136) [hereinafter Digital Content Directive].

41. 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) 1 [hereinafter Digital Services Act].

legislation (e.g., on personal data protection, privacy, or competition law) so long as it is relevant to consumer protection law provisions. Otherwise, legislation that does not intersect with consumer law provisions is outside of the scope of this Article. Moreover, in addition to the provisions themselves, this Article references case law, publications of regulatory authorities, and academic literature to illuminate how the provisions are currently understood and practiced. Additionally, the Article incorporates the technical, economic, and societal aspects of targeted advertising and the application of the relevant legal provisions in these areas.

The targeted advertising ecosystem and market are complex, and to elaborate on the extent to which they are limited, a description of the practices and their technical underpinnings is necessary. With this aim in mind, Part II of the Article sheds some light on what targeted advertising is and how it works. Part III analyzes the EU's legal framework for consumer protection for targeted advertising. Firstly, Part III.A provides an overview of consumer protection legislation and maps out how it limits targeted advertising in two stages: first, when consumers enter into contracts with publishers that monetize their digital content or services via targeted advertising (contracting stage) and, second, when consumers are presented with a personalized advertisement (advertising stage). Part III.B analyzes consumer protection laws in the contracting phase, and Part III.C for the advertising stage. Moreover, Part III.D addresses central challenges and gaps in consumer protection law that the Commission may want to consider in its re-thinking of consumer protection regulation to better address the challenges of the digital age.

II. TARGETED ADVERTISING

To discuss the limitations of European consumer protection law on targeted advertising, it is critical to understand what targeted advertising is and how it works. This is especially important given that there are several similar concepts and terms that overlap in the legal doctrine and in the business practices of targeted advertising. Therefore, first, Part II.A examines what targeted advertising is and delineates this term. Second, Part II.B discusses how targeted advertising works. Together, this provides the foundation for the discussion on consumer protection law in the EU that follows in PartIII.

A. *What Is Targeted Advertising?*

Targeting practices in marketing are not new phenomena and are not limited only to the digital environment. The Nielsen ranking system developed in the 1940s for radio and expanded for television in the 1950s provided audience measurements that advertisers used (and still use) to target their preferred groups by selecting particular radio

and television programs to insert their commercials.[42] Since the rise of digital technologies and the ability of companies to process larger amounts of data about consumers, more nuanced targeting practices have emerged. In particular, supermarkets have been pioneers in data-driven targeted marketing.[43] Target, an American store, made headlines in 2012 when through data mining practices, it predicted the pregnancy of a consumer and sent her marketing booklets for diapers.[44] Nevertheless, the advance of the internet provided online platforms unprecedented capability to surveil and segment audience and has turned targeted advertising into the central business model of the internet.

This Article refers to targeted advertising as an online marketing practice that delivers an advertisement—explicitly sponsored marketing communication—to a particular consumer based on data collected from the consumer or the content of a "publisher" (i.e., provider of digital service or content).[45] One subtype of this practice is "contextual advertising," which targets consumers based on the context, including the publisher's content or the central theme of the web page or app.[46] Such targeting may also include data about the country the digital content is accessed from, as well as its language.[47] For example, suppose a consumer residing in the Netherlands is reading a blog in the English language about the benefits of running. In that case, contextual advertising may expose them to advertisements in English for running shoes that can be bought and delivered in the Netherlands. Moreover, contextual advertising is

---

42. *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 38–39 (2019).

43. *See* JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 1–2, 64–65 (2017).

44. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/6G3T-UCQK] (archived Feb. 7, 2023).

45. *See* EUR. COMM'N, CONSUMER MARKET STUDY ON ONLINE MARKET SEGMENTATION THROUGH PERSONALISED PRICING/OFFERS IN THE EUROPEAN UNION 31, 41 (2018) [hereinafter EC MARKET STUDY ON PERSONALISATION]. There are various online marketing strategies, such as search engine optimization (SEO), that can increase the chances of showing the link on top, as well as influencer marketing that is prominent in social media and video streaming websites. Such marketing strategies are also associated with consumer harm, and consumer protection rules would apply in their context. Therefore, this article excludes any direct discussion of these practices.

46. *See Contextual Targeting*, GOOGLE, https://support.google.com/google-ads/answer/1726458?hl=en (last visited Mar. 12, 2023) [https://perma.cc/F8HL-3WPE] (archived Feb. 7, 2023).

47. Contextual advertising in general does not rely on 'personal data' as defined by the General Data Protection Regulation. Nevertheless, such personal data can be used, for example, for *frequency capping*—capping how many times specific user sees an ad. *See* EU Directorate-General for Internal Policies, Pol'y Dep't for Citizens' Rights & Const. Affs., Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent, PE 694.680, at 26 n. 20 (2021) [hereinafter EU Report Targeted Advertising & Informed Consent].

becoming more sophisticated and may use AI to analyze digital content and assess who the likely reader is.[48] On the other hand, "personalized advertising" targets individual consumers based on the data about consumers themselves.[49] Targeting in personalized advertising is granular and can be further categorized based on the nature of the information used for segmenting the consumer audience.

"Broad targeting" (alternatively "broad demographic targeting," or "demographic targeting")[50] uses the information that consumers voluntarily provide when they sign up for digital services or digital content, and it usually includes their gender, age, and country of residence.[51] For example, in order to promote its business, an exclusively women's fitness studio located in a particular city may choose to target women between ages of eighteen to sixty-five who live in that city and the surrounding area. Moreover, personalized advertising can take the form of more *detailed demographic targeting*, where the consumer audience is narrowed down by their education (e.g., high-school graduate), finances (e.g., household income in the top 10 percent), relationship status (e.g., married), parental status (e.g., parent of two), employment (e.g., tech industry) or other socio-demographic categories.[52] While broad targeting relies solely on the information that the consumers voluntarily provided, detailed demographic targeting can be based on the data that was *observed* about the consumer (captured when tracking a consumer across the internet), as well as data that was *inferred* about them (via analyzing

48. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 159.

49. *See Personalized Advertising*, GOOGLE, https://bit.ly/3SSOTIT (last visited Feb. 7, 2023) [https://perma.cc/WKW5-PF33] (archived Feb. 7, 2023).

50. Note that broad demographic targeting is often referred to as *segmented targeting*, in particular by the EU institutions. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 31; EU Pol'y Report Online Advertising, *supra* note 19, at 19; EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 24, 50. This is done with the purpose of differentiating targeting based on the data consumers voluntarily provide (age, gender, country of residence) from *behavioral targeting*, where the data is often inferred, observed, and derived from consumers' behavior. However, even in such cases, consumer profiles are built for segmentation—splitting them into groups based on some characteristics. To avoid confusion, this Article differentiates between *demographic targeting* (broad targeting or broad demographic targeting) and *detailed demographic targeting*, a sub-category of *behavioral targeting* that also includes affinity (interest) targeting.

51. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 24, 31; *About Demographic Targeting*, GOOGLE, https://support.google.com/google-ads/answer/2580383 (last visited Feb. 7, 2023) [https://perma.cc/SSU6-VDBM] (archived Feb. 7, 2023).

52. *See About Demographic Targeting*, *supra* note 51; *About Detailed Targeting*, META, https://www.facebook.com/business/help/182371508761821 (last visited Feb. 19, 2023) [https://perma.cc/AA8Y-P8JB] (archived Mar. 28, 2023).

and combining different parameters).[53] Combining such data about the consumer is often referred to as "profiling."[54]

Personalized advertising that is based on the profiling of consumers is also called "behavioral advertising" (or "online behavioral advertising").[55] In behavioral advertising, beyond demographic traits, consumers can be segmented according to their behavior and affinity or *psychographic* traits (e.g., interest, values, or lifestyle).[56] Targeting based purely on consumers' online behavior is called "re-targeting"—when consumers receive an advertisement for the products and services in which they revealed interest by, for example, adding them into the shopping cart of the online marketplace.[57] Consumers experience re-targeting as being followed by advertisements across the internet.[58] For example, consumers who were 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 they have moved on from the club's website and are now reading an online newspaper, or checking their social media feeds.

However, behavioral advertising goes beyond mere re-targeting and uses consumers' behavioral data (e.g., among others, data about the posts on social media, search history, and browsing history) to infer their interests, values, and lifestyles.[59] The single consumer can be profiled with hundreds of variables such as being a "surf enthusiast," a "sci-fi fan," "a dog lover," someone who "is about to have a wedding anniversary," or someone who "recently moved to Hawaii."[60] Moreover, for behavioral advertising, consumers can profile based on their similarity with other consumers ("look-alike audience").[61] For example, it can be inferred that someone is in a relationship because people with very similar browsing histories have also disclosed that they are in a relationship. Finally, behavioral advertising can include broad

53. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 49.

54. The GDPR 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." General Data Protection Regulation, *supra* note 23, art. 4(4).

55. *See* FREDERIK J. ZUIDERVEEN BORGESIUS, IMPROVING PRIVACY PROTECTION IN THE AREA OF BEHAVIOURAL TARGETING 15 (2015).

56. *See About Audience Targeting*, GOOGLE, https://support.google.com/google-ads/answer/2497941?hl=en (last visited Feb. 7, 2023) [https://perma.cc/SQ5N-8MXZ] (archived Feb. 7, 2023).

57. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 19.

58. *See id*. at 19–20.

59. *See id*. at 19.

60. *See About Demographic Targeting*, *supra* note 51.

61. *See About Similar Audiences for Search*, GOOGLE,https://support.google.com/google-ads/answer/7151628 (last visited Feb. 7, 2023) [https://perma.cc/5BF7-E3H4] (archived Feb. 7, 2023); *About Lookalike Audience*, META,https://www.facebook.com/business/help/164749007013531 (last visited Aug. 16, 2022) [https://perma.cc/WAA9-CVQV] (archived Mar. 28, 2023).

demographic or contextual targeting to enable further optimization and more fine-grained personalization of targeted advertisement.[62]

Moreover, personalization based on the profiling in the digital environment can take other forms, such as "personalized ranking" or "personalized pricing," both of which can be entirely different practices, but also forms of personalized advertising if they are sponsored by advertisers.[63] Personalized ranking (alternatively "personalized offers," or "personalized ranking of offers") is a practice that relates to changing the order of offers, usually search results, to highlight specific content, services, or products, when consumers search for them online.[64] Personalized ranking characterizes digital content or services that allow searches, such as search engines, but also online marketplaces and video-streaming platforms. For example, a consumer searching for "boxing gloves" on the online marketplace will be presented with offers from different suppliers. In the ranking of offers, prominence is given to suppliers from which the consumer has already bought other products. Some of these publishers allow advertisers to pay for the prioritization of their products in ranking.[65] This Article only covers personalized ranking to the extent that the advertisers pay for a higher ranked position ("paid ranking") and therefore is a form of personalized advertising.[66]

"Personalized pricing" (or "price discrimination") refers to the practice of "differentiating the online price for identical products or services partly based on information a company has about a potential customer."[67] Similar to paid ranking, this Article only covers personalized pricing to the extent to which it is incorporated within

---

62. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 20.

63. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 33.

64. Personalized ranking is sometimes also referred to as *price-steering*, which is only its sub-type, and refers to the personalization of ranking to influence consumer's willingness to pay a price by placing "more or less expensive products at the top of the list." *See* Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove & Christo Wilson, *Measuring Price Discrimination and Steering on E-commerce Web Sites*, *in* IMC '14: PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT CONFERENCE 305, 307 (2014). Nevertheless, such influence is only one of several reasons why ranking can be personalized, including likelihood of consumer making a purchase. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 42–43 (discussing how companies have begun to use personalized ranking of offers to steer certain customers towards pricier products, such as for hotels and entertainment tickets, though the practice remains in experimentation).

65. *See Commerce Ranking Disclosure*, FACEBOOK, https://www.facebook.com/legal/commerce_ranking (May 28, 2022) [https://perma.cc/73K4-Y72U] (archived Feb. 7, 2023).

66. *See* European *Commission Notice, Guidance on Ranking Transparency Pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council*, 2020 O.J. (C 424) 6–7 [hereinafter *Guidance on Ranking Transparency*].

67. Frederik Zuiderveen Borgesius & Joost Poort, *Online Price Discrimination and EU Data Privacy Law*, 40 J. CONSUMER POL'Y 347, 348 (2017); *see also* Sears, *supra* note 31, at 3.

personalized advertising, such as when consumers are offered personalized discounts based on their previous buying history.[68]

B. *How Does Targeted Advertising Work?*

Targeted advertising is displayed by the "publishers"—the providers of digital services and content that monetize consumer visits by selling advertising space (i.e., inventory) to advertisers.[69] While the large advertisers (e.g., L'Oreal, Unilever, Proctor & Gamble) are responsible for most of the spending, targeted advertising is accessible to many small advertisers globally, including individuals.[70] Similarly, there are small publishers (e.g., individuals running blogs) and large publishers, such as games (e.g., Candy Crush Saga, Pokémon Go, etc.) and news media (e.g., *the Guardian*, *the New York Times*, etc.).[71] However, the largest publishers are the online platforms (e.g., Google, Facebook, etc.) that act as gatekeepers to the internet and can reach the most consumers online.[72] For example, Google manages 90 percent of all searches in Europe, and Meta's platforms (Facebook and Instagram) handle 80 percent of all social network traffic worldwide.[73] Because of their reach, these platforms are best equipped to segment massive consumer bases into narrowed-down target audiences (i.e., render consumers legible) and provide advertisers with access to them.[74]

---

68. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 63.

69. *See Glossary of Terminology*, INTERACTIVE ADVERT. BUREAU, https://www.iab.com/insights/glossary-of-terminology/ (last visited Feb. 19, 2023) [https://perma.cc/S9YV-TF6X] (archived Feb. 19, 2023) [hereinafter iab Glossary].

70. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 61.

71. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 26.

72. *See* Cohen, *supra* note 15, at 8. For another example, in 2020, UK internet users spent 50 percent of their time online on just ten platforms. *See* COMPETITION AND MKT. AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING, APPENDIX C: MARKET OUTCOMES C11 (2020) [hereinafter APPENDIX C].

73. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 19; *see also* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 336–37. As a comparison, 37 percent of all internet traffic was handled by platforms of Google and Meta combined (Google—24 percent, Meta—13 percent). Also, in the U.K., Google has more than 90 percent of the search market, and reaches 90 percent of all internet users. Meta (with its Facebook, Instagram, and WhatsApp platforms) has a reach of 85 percent of all internet users, and 75 percent of their time on social media. *See* APPENDIX C, *supra* note 72, at C11. Google and Meta run four out of the five most visited websites. *See Top Website Ranking*, SIMILARWEB, https://www.similarweb.com/top-websites/ (last visited Feb. 19, 2023) [https://perma.cc/9XG3-T4K5] (archived Feb. 19, 2023); *see also Most Popular Websites Worldwide as of November 2022*, STATISTA (Feb. 9, 2023), https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/ [https://perma.cc/8WDE-RCGG] (archived Feb. 9, 2023).

74. *See* Cohen, *supra* note 15, at 6.

Therefore, online platforms are the primary beneficiaries of targeted advertising.[75] For illustration, more than 80 percent of global targeted advertising revenue goes to large online platforms and more than 60 percent to platforms operated by Google and Meta.[76] In the United Kingdom, platforms of Google and Meta received 80 percent of targeted advertising revenue in 2019.[77] Due to such a large market share, *on-platform* and *off-platform* advertising are often discussed separately.[78] On-platform targeted advertising includes search advertising (also keyword advertising),[79] social network advertising, and video-on-demand advertising.[80]

The fundamental premise in targeted advertising, in particular *on-platform*, is that ability of consumer segmentation can be used to show *relevant* advertisements and, therefore, minimize waste in advertising expenditure.[81] This potential to eliminate waste is actualized by the ability of online platforms to observe if consumers take action on the particular advertisement (i.e., click-through rate, or CTR[82]) and, therefore, to measure the optimization of the "matching" process—a feat that was unattainable in conventional, non-digital outlets on television, radio, print, and billboards.[83] With a presumed

---

75. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 35; *see also* Cohen, *supra* note 15, at 8.

76. Google and Meta are often referred to as a "duopoly" (or quasi-duopoly) in the targeted advertising market. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 39; *see also* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 41–43. However, Amazon has recently been raising its targeted advertising revenue, and, therefore, there have been new references to a "triopoly" as well. *See* Forrester, *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/?sh=2effcee86343 [https://perma.cc/YZ4A-5BDR] (archived Feb. 11, 2023).

77. CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 10.

78. *See* EC MARKET STUDY ON PERSONALISATION, *supra* note 45, at 23; EU Pol'y Report Online Advertising, *supra* note 19, at 17; CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 60; EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 31.

79. Search advertising usually takes the form of a sponsored hyperlink that is presented on top of the search results for the consumer's query. Adverts may also appear, for example, in users' queries on maps. More than 60 percent of all on-platform advertising is search advertising, more than 80 percent of which goes to Google. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 16.

80. Video advertising is delivered within web- or app-based video streaming online platforms, such as YouTube, Vimeo, etc. Advertisements can take the form of a video (e.g., pre-roll advertisements), text, or an image overlay. This segment accounts for 9.4 percent of the revenue of the global online advertising market and is dominated in the United States and Europe by Google (which owns and operates YouTube*). See* EU Pol'y Report Online Advertising, *supra* note 19, at 17.

81. *See id*. at 18.

82. *Clickthrough Rate (CTR): Definition*, GOOGLE, https://support.google.com/google-ads/answer/2615875?hl=en&ref_topic=24937 (last visited Feb. 11, 2023) [https://perma.cc/A475-LNLN] (archived Feb. 11, 2023).

83. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 18.

ability to meet the demands of such optimization imperative, behavioral advertising introduced by Google emerged as the most profitable and, therefore, most prominent model in targeted advertising.[84]

Behavioral advertising models, extracts, and processes consumers' behavioral data ("behavioral surplus," or "data exhaust") to create fine-grained consumer profiles. Moreover, it feeds these data to AI systems to predict "quality scores," which estimate click-through rates or the likelihood of consumers reacting to the advertisement.[85] Online 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.[86] In most cases, in behavioral advertising, advertisers pay per action ("cost-per-action"), such as a click on the advertisement ("cost-per-click," or CPC). Therefore, bids refer to the amount of money advertising is willing to pay per click.[87] At the time of advertisement impression (that is, when a consumer visits a page with pre-defined advertising space) the online platform initiates a real-time and programmatic (fully automated) process designed to maximize the platform's profits by matching consumers with advertisements based on the "quality score" and advertisers' bids.

Moreover, with advanced analytic tools, platforms allow advertisers to observe how consumers behave regarding their advertisements and enable them to further tailor their campaigns based on these insights, creating a self-improving optimization cycle.[88] Note that while general criteria of programmatic auctions are known, and analytics tools enable optimizing the campaigns for advertisers, algorithms that underlie these processes are largely a black-box—and remain unexplainable.[89] Nevertheless, it is data about the consumers and their behavior that fuels programmatic advertising and determines the efficacy of ad optimization.[90]

Online platforms also expand their behavioral advertising practices beyond their platforms by creating "advertising networks," such as Google's AdSense and AdMob, Meta's Audience Network, and

---

84. It is estimated that the CTR of behavioral advertising is 5.3 times higher than broad demographic targeting. *See id.* at 19.

85. *See About Quality Score*, GOOGLE, https://support.google.com/google-ads/answer/6167118?hl=en (last visited Feb. 11, 2023) [https://perma.cc/JMG8-BHU3] (archived Feb. 11, 2023).

86. *See Estimate Your Results with Bid, Budget and Target Simulators*, GOOGLE, https://support.google.com/google-ads/answer/2470105?hl=en&ref_topic=3122864 (last visited Feb. 11, 2023) [https://perma.cc/3W83-GCK7] (archived Feb. 11, 2023).

87. *Id.*

88. *See* ZUBOFF, *supra* note 32, at 93–97.

89. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 16.

90. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 18.

Amazon Publisher Services.[91] By creating advertising networks, online platforms also act as advertising intermediaries between advertisers and other publishers that are unable to provide similar advertisement optimization independently.[92] Such expansion increases the profit of online platforms, not only via expanding the reach for their advertisers but also because they can now collect consumer data beyond their media and on the sites and apps of the publishers within their advertising networks. The most prevalent way to track the user over the advertising network is by placing trackers, also known as third-party tracking cookies.[93]

Cookies are small blocks of data placed on a user's computer for various purposes when visiting a website. First-party cookies are set by the server of the publisher's website that is being visited. These cookies can be strictly necessary for enabling features of the website (e.g., for accessing secure areas or adding items to a shopping cart), they can be used to improve performance (e.g., to track errors or which pages of the website are most visited), or they can enable other functionalities (e.g., keeping login status, retaining preferences and region) in addition to enabling personalization or tracking.[94] There are also third-party cookies, which are placed by a third party via code loaded on the publisher's website. These are primarily used by advertisement networks in order to collect user information to be used in their targeting advertising practices.[95] Moreover, as advertising networks place third-party cookies through the websites of many different publishers, they can aggregate a vast amount of data regarding a single individual and build comprehensive profiles.[96] Consumers visiting publisher's websites are not always aware that third parties observe their behavior, raising concerns about consumer privacy.[97]

---

91. "Advertising network" is an advertising intermediary that provides advertisers with the advertising spaces aggregated from publishers and consumer target audiences. *See* GLOSSARY OF TERMINOLOGY, INTERACTIVE ADVERT. BUREAU, https://www.iab.com/insights/glossary-of-terminology/ (last visited Feb. 19, 2023) [https://perma.cc/YC53-J62K] (archived Feb. 19, 2023).

92. *See* ZUBOFF, *supra* note 32, at 93–97.

93. *See* Veale & Borgesius, *supra* note 18, at 227–29.

94. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 44; 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/ [https://perma.cc/D3YK-CZ28] (archived Feb. 9, 2023).

95. *See* Frederik Brau, Origin Policy Enforcement in Modern Browsers 28–29 (Oct. 26, 2012) (Diploma thesis, Ruhr-Universität Bochum).

96. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 44.

97. *See* Brau, *supra* note 95, at 37. The Same Origin Policy governing cookies was developed to ensure web browser security by allowing only one server to place cookies from each browsing page. Advertising networks are able to place cookies, as they "own" so called *frames* on the websites of the publishers, that are different circumvented the Same Origin Policy by using a frame function to own elements on the publisher's website,

Another technology used for tracking is called a "web beacon."[98] Web beacons often use single-pixel images (or 1x1 pixels) in order to collect data on website users, and they can be self-hosted or hosted by third-party servers.[99] These pixels are usually invisible to users, not only due to their extremely small size but also because they usually make use of the same color as the background or are transparent.[100] In addition to being incorporated into advertisements, web beacons can also be used in emails, and social media websites have incorporated web beacons into clickable buttons. As an example, when a user's browser requests to load the 1x1 pixel image, certain data is collected; this typically includes the user's IP address, the time of the request, information about the browser or email application making the request, and whether there are cookies that have been previously set by the server hosting the pixel image.[101] Web beacons can also be used to deliver cookies,[102] and the data collected can often be combined with data gathered from other sources.[103] While cookies can be controlled to an extent through browser settings, the same is not possible for web beacons.[104]

Given the control of cookies afforded by browsers, advertisers and trackers began to look for other ways to connect users with their browsing records; companies began to offer such services as early as 2009.[105] Device fingerprinting is one of the core inferred methods used for tracking users.[106] At a basic level, when a user's browser or device requests information from the website's host server or from the server providing information for an app, certain information is collected. This usually includes the user's device, operating system, screen resolution,

---

placing a cookie, and attaching the unique identifier to a consumer. This form of tracking was known as a 'third-party cookie.' *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 43–44.

98. Web beacons are also known 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. DIGIT. HUMANITIES 65, 67 (2021); David Martin, Hailin Wu & Adil Alsaid, *Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use*, 46 COMMC'NS OF THE ACM 258, 259 (2003).

99. *See* Nielsen, *supra* note 98, at 66; *see also* NETWORK ADVERT. INITIATIVE, WEB BEACONS–GUIDELINES FOR NOTICE AND CHOICE 2 (2004).

100. *See* Nielsen, *supra* note 98, at 66.

101. *See* Richard M. Smith, *The Web Bug FAQ*, ELEC. FRONTIER FOUND. (Nov. 11, 1999), https://w2.eff.org/Privacy/Marketing/web_bug.html [https://perma.cc/KK46-UGGB] (archived Feb. 12, 2023).

102. *See* NETWORK ADVERT. INITIATIVE, *supra* note 99, at 2.

103. *See* Nielsen, *supra* note 98, at 66.

104. *See* Alexandre Fortier & Jacquelyn Burkell, *Hidden Online Surveillance: What Librarians Should Know to Protect Their Privacy and That of Their Patrons*, 32 INFO. TECH. LIBRS. 59, 64 (2015).

105. *See* Nick Nikiforakis, Alexandroz Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens & Giovanni Vigna, *Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting*, 2013 IEEE SYMP. ON SEC. & PRIV. 541, 541 (2013).

106. *See* NETWORK ADVERT. INITIATIVE, *supra* note 99, at 2.

browser and browser version, language, and time zone,[107] which can then be used (and often combined with other data) to build profiles of users. This information can be used to re-identify the user via primarily probabilistic means. For example, suppose the user clears their cookies. In that case, the fingerprinting approach can respawn deleted identifiers.[108] Fingerprinting is also a way to enable cross-device tracking (even without having two devices logged in to the same service, for example, the same router).[109] The research found fingerprinting evidence on at least 4.4–5.5 percent of top websites.[110]

An amendment to the ePrivacy Directive in 2009 required users' informed consent to use cookies and other similar technologies.[111] In practice, to comply with this requirement, publishers have employed so-called cookie banners that appear when users visit the publisher's website for the first time, asking them to accept cookies and other technologies for various purposes.[112] This placement of cookies for tracking is what has enabled targeted advertising—a 2015 study of 478 websites across eight member states found that 70 percent of the 16,555 cookies placed were third-party cookies, and more than half of those were set by only twenty-five domains.[113] Some software developers recognized the threat to users' privacy and started disabling third-party cookies by default, such as Mozilla's Firefox in 2019 and Apple's Safari in 2020.[114] Many websites and consent management

---

107. Much of this information is obtainable using HTTP headers, although some require JavaScript.

108. *See* Veale & Borgesius, *supra* note 18, at 21; *see also* Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan & Claudia Diaz, *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 674 (ACM 2014).

109. *See* Veale & Borgesius, *supra* note 18, at 230.

110. *Id*.

111. *See* ePrivacy Directive, *supra* note 22, art. 5(3); *Opinion 9/2014 of the Article 29 Data Protection Working Party on the Application of Directive 2002/58/EC to Device Fingerprinting*, 2014 WP 224 at 3; *see also* Directive 2009/136/EC, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services 2009 O.J. (L 337) ¶ 28; Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) art. 2(5). It should be noted that the effective date for member states was generally in 2011, with a number of countries implementing the Directive several years later. *See generally* EU LAW ON COOKIES, DLA PIPER (2020).

112. This includes both first and third-party cookies, as well as for other tracking technologies discussed above.

113. *Report of Article 29 Data Working Party on the Cookie Sweep Combined Analysis*, at 2, WP (2014) 229 final (Feb. 3, 2015) [hereinafter *Cookie Sweep Report*].

114. *See* Marissa Wood, *Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, MOZILLA (Sept. 3, 2019), https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/ [https://perma.cc/L9YE-58XU] (archived Feb. 19, 2023); 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 [https://perma.cc/8V2D-NAH5] (archived Feb. 11, 2023).

platforms (CMPs) design cookie banners in such a way so as to nudge users into accepting tracking cookies and other technologies (such practices are often referred to as "dark patterns").[115] For example, users may be presented with a colorful "accept all" button versus a nondescript "see cookie settings" link, the latter of which they must click in order to save their preference, declining the use of cookies, and thus there is substantially more friction.[116] This is compounded when the website, upon repeat visits, prompts the user to save their preference declining cookies every time they visit, yet if they accept, the cookies will be saved on the user's computers for years and users are not prompted again.[117] Another tactic that was widely used was pre-ticking consent boxes, which persisted until, and shortly after, the *Planet49* case was decided in late 2019.[118] However, even well after this case, perhaps the largest CMP was boasting of obtaining above a 90 percent average consent rate.[119] More recently, a number of CMPs and websites have shifted towards using pre-ticked "legitimate interest" as opposed to consent in order to place cookies and other technologies.[120] However, these other technologies may take a more prominent position after Google's Chrome—which has 65 percent of the

115. *See* Philip Hausner & Michael Gertz, Dark Patterns in the Interaction with Cookie Banners (May 2021) (position paper at the CHI Conference on Human Factors in Computing Systems in Yokohama, Japan). While dark patterns can be used in a variety of circumstances in digital environments (e.g., to unsubscribe from services), this Article focuses on dark patterns solely used for coercing or manipulating users to consent to data processing, or to enter a contract with the publisher that monetizes its services via targeting advertising.

116. *See id.*; Esther van Santen, Presentation at the Seventeenth International Multi-Conference on Computing in the Global Information Technology, Cookie Monsters on Media Websites: Dark Patterns in Cookie Consent Notices, (May 2022), https://www.iaria.org/conferences2022/filesICCGI22/ICCGI_18003.pdf [https://perma.cc/GBF4-UTXF] (archived Mar. 28, 2023).

117. In some cases, the cookie retention period is set at nearly eight thousand years. *See Cookie Sweep Report*, *supra* note 113, at 2.

118. *See* Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände—Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, ECLI:EU:C:2019:801, ¶ 62 (Oct. 1, 2019) [hereinafter *Planet49*].

119. *See Quantcast Choice Powers One Billion Consumer Consent Choices in Two Months Since GDPR*, QUANTCAST (July 31, 2018), https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/ [https://perma.cc/7BXH-E8AP] (archived Feb. 9, 2023).

120. *See* Thea Felicity, *Top 5 Best Consent Management Platforms in 2022 To Easily and Legally Manage User Data*, TECH TIMES (Mar. 8, 2022), https://www.techtimes.com/articles/272671/20220308/top-5-best-consent-management-platforms-in-2022-to-easily-and-legally-manage-user-data.htm [https://perma.cc/VP4Q-T5WE] (archived Feb. 12, 2023).

market[121]—follows suit in disabling third-party cookies in 2023, despite owing much of their success to this method.[122]

Advertising networks of online platforms providing off-platform targeted advertising are often referred to as "walled gardens"—closed ecosystems in which platforms provide complete end-to-end technical solutions for advertisers and publishers.[123] However, the demand of some (mostly large) advertisers and publishers to have more control of the advertising processes (e.g., by connecting to several advertising networks) triggered the emergence of an entire *off-platform open display advertising* market with smaller advertising intermediaries facilitating different aspects of the advertising process.[124] Demand side platforms (DSPs) provide advertisers with a one-stop platform for buying advertisements from many other sources.[125] Supply-side platforms (SSPs) aggregate publishers' advertising space similarly to advertising networks, but they serve publishers exclusively.[126] "Advertising servers" provide services to advertisers and publishers for them to track, manage, and measure advertising campaigns.[127] Advertisers' ad servers offer a centralized tool for managing their campaigns, including uploading "ad-creatives" or advertising designs for a particular advertisement in the campaign, setting targeting criteria, or measuring performance goals across various DSPs.[128] 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.[129]

These advertising intermediaries connect via "advertising exchanges"—platforms that provide sales channels and facilitate a

---

121. *Browser Market Share Worldwide*, STATCOUNTER, https://gs.statcounter.com/browser-market-share (last visited Feb. 12, 2023) [https://perma.cc/BFX9-X2JK] (archived Feb. 12, 2023).

122. *See* Dieter Bohn, *Google Delays Blocking Third-Party Cookies in Chrome Until 2023*, THE VERGE (June 24, 2021), https://www.theverge.com/2021/6/24/22547339/google-chrome-cookiepocalypse-delayed-2023 [https://perma.cc/Z7HR-9DLB] (archived Feb. 11, 2023). Google plans to launch its Privacy Sandbox as a replacement. *See* Mat Burgess, *Google Has a New Plan to Kill Cookies. People Are Still Mad*, WIRED (Jan. 27, 2022), https://www.wired.com/story/google-floc-cookies-chrome-topics/ [https://perma.cc/A3AC-8C9Q] (archived Feb. 11, 2023).

123. CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 155.

124. *See id*. at 263–65.

125. *See* iab Glossary, *supra* note 69.

126. *See id*.

127. *See id*.

128. *See Introducing Campaign Manager 360*, GOOGLE, https://support.google.com/campaignmanager/answer/10157783?hl=en&ref_topic=2758513 (last visited Feb. 12, 2023) [https://perma.cc/EQD7-AP4J] (archived Feb. 12, 2023).

129. *See Advertising with Google Ad Manager*, GOOGLE, https://support.google.com/admanager/answer/6022000?hl=en (last visited Feb. 12, 2023) [https://perma.cc/9CHP-DC6Z] (archived Feb. 12, 2023).

real-time programmatic auction process through which advertising space is sold and bought.[130] Ad exchanges differ from ad networks, as in their real-time bidding auction process, they can connect ad networks and other advertising intermediaries.[131] When a consumer visits a publisher's website, an advertising tag within the browsing window triggers the submission of an ad request to the publisher's ad server that places a tag on the website.[132] An ad request contains extensive information about the consumer, and the advertising space notifies SSPs about the availability for ad placement.[133] SSPs pass on ad requests to multiple DSPs that evaluate advertising opportunities based on their campaign objectives and respond with their bids.[134] SSPs then rank the bids based on the price and priorities of the publisher.[135] Further, the publisher's ad server compares bids and decides which advertisement will be served on the webpage. Similar to on-platform advertising, ad exchange real-time bidding is set up to maximize advertisement quality (estimated likelihood of consumer acting on the ad). In addition, data management platforms have emerged that compile data from various suppliers and enrich advertising intermediaries by providing platforms that enable them to target more narrowed-down consumer audiences.[136]

Finally, to facilitate a myriad of intermediaries that share consumer data with each other, advertising intermediaries not only use third-party cookies but also engage in *cookie syncing* (also known as *cookie matching*)—a process by which several third parties can associate separate unique identifiers related to one consumer.[137] Cookie syncing significantly widened the scope of tracked activity

---

130. *See* iab Glossary, *supra* note 69.

131. *See id.*

132. *See Ad Selection White Paper*, GOOGLE, https://support.google.com/admanager/answer/1143651 (last visited Feb. 12, 2023) [https://perma.cc/UXR7-S9RZ] (archived Feb. 12, 2023).

133. There are two prominent protocols of "ad requests' requests" or "bid requests' requests" in the market: Google's Authorized Buyers and IAB's OpenRTB standards. Usually, bid requests contain the following information: site, url of the site visited, site category or topic, device, operating system, browser software and version, device manufacturer, model, mobile provider, screen dimension, user, unique identifiers set by vendors and/or buyer, year of birth, gender, interests, metadata reporting on consent, geography, longitude and latitude, postal code, etc. *See Authorized Buyers Real-Time Bidding Proto*, GOOGLE, https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide (last visited Feb. 12, 2023) [https://perma.cc/TAL7-QV6X] (archived Feb. 12, 2023); *see also OpenRTB Integration*, GOOGLE, https://developers.google.com/authorized-buyers/rtb/openrtb-guide (last visited Feb. 12, 2023) [https://perma.cc/LX9Q-UNGA] (archived Feb. 12, 2023).

134. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 265.

135. *See id.* at 265.

136. *See id.* at 155.

137. *See* Veale & Borgesius, *supra* note 18, at 229.

online by pooling the reach of multiple trackers.[138] Moreover, CMPs serving non-platforms advertising intermediaries made use of the Interactive Advertising Bureau's Transparency and Consent Framework (TCF), which aims to aid their compliance with the GDPR.[139] However, in February 2022, the Belgian Data Protection Authority issued a decision that may require the fundamental reconstruction of the TCF.[140] In September 2022, the Belgian Data Protection Authority referred the case to the Court of Justice of the European Union (CJEU) with the request for a preliminary ruling on this matter.[141]

It can be argued that the programmatic processes described above are not necessary for conducting targeted behavioral advertising. For example, a method for developing a plug-in that builds a consumer profile all within the user's device, without sharing any data between third parties, was proposed in 2010.[142] However, privacy-preserving technologies have only been implemented to a limited extent because they may lose some benefits of using personal data, do not align with business objectives, or lack technical expertise.[143] Nonetheless, such

---

138. Research shows that fifty-three companies observe more than 91 percent browsing behavior of all internet users. Advertising companies tracking spreads across entire internet. *See id.* at 228.

139. TCF framework collects and transmits signals of consent from an individual to third party vendors. Site and app operators provide disclosures and seek consumers' consents through a CMP and pass this through the supply chain. IAB Europe maintains a list of registered and compliant CMPs and a Global Vendor List (GVL), of all registered and approved third parties ('Vendors') participating in the TCF. *See id.* at 244.

140. This relates to considering user's cookie preferences as personal data; therefore, asserting joint controllership of with regards to processing of such data to IAB Europe, that would require them an extra consent for each time it shares such information with other third parties. In practice, that may be an impossible ask. *See* Michael Veale, Midas Nouwens & Cristiana Santos, *Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?*, TECH. & REG. 12, 12 (2022); *see also Belgian DPA ("APD") Decision on IAB Europe and the TCF: IAB Europe Submits Action Plan, A Key Milestone in the Process*, IAB EUR. (April 1, 2022), https://iabeurope.eu/all-news/belgian-dpa-apd-decision-on-iab-europe-and-the-tcf-iab-europe-submits-action-plan-a-key-milestone-in-the-process/ [https://perma.cc/2WYH-6667] (archived Feb. 2, 2023).

141. *See IAB Europe case: The Market Court refers preliminary questions to the Court of Justice of the EU*, AUTORITÉ DE PROTECTION DES DONNÉES GEGEVENSBESCHERMINGSAUTORITEIT [BELGIAN DATA PROTECTION AUTHORITY] (Sept. 7, 2022), https://dataprotectionauthority.be/citizen/iab-europe-case-the-market-court-refers-preliminary-questions-to-the-court-of-justice-of-the-eu [https://perma.cc/SNG6-MP86] (archived Feb. 2, 2023).

142. *See* Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum & Solon Barocas, *Adnostic: Privacy Preserving Targeted Advertising*, Proceedings of the Network and Distributed System Symposium (2010), https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf [https://perma.cc/V64V-HJXB] (archived Feb. 2, 2023).

143. *See* Micah Altman, Alexandra Wood, David O' Brien & Urs Gasser, *Practical Approaches to Big Data Privacy Over Time*, 8(1) INT'L DATA PRIVACY L. 29, 29 (2018); *see also* Daniel Bachlechner, Karolina La Fors & Alan M. Sears, *The Role of Privacy-Preserving Technologies in the Age of Big Data*, Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, WISP 2018, at 9.

techniques are slowly entering practice, such as with Google's Federated Learning of Cohorts system for microtargeting within Chrome.[144] Furthermore, off-platform advertising is not limited to personalized advertising. In contextual advertising, ad networks provide an advertiser with a choice of content topics or the possibility to enter custom keywords, such as "benefits of running."[145] In this case, ad networks scan various publishers' websites. Instead of consumer information, it analyzes the attributes of digital content of all the publishers it serves (e.g., text, link structure, and pictures) and, as a result, provides the advertiser with an ad inventory.[146]

While the open display market is characterized by complexity and a myriad of advertising intermediators, it amounts to only 15 percent of the targeted advertising market.[147] Even then, providers of online platforms, notably Alphabet (Google) and Meta (Facebook), provide the largest advertising intermediaries in all their functions.[148] Google's AdSense and AdMob are the most prominent advertising networks.[149] Google's Ad Manager is not only the largest SSP but also the largest ad server.[150] Google's Authorized Buyers is the largest ad exchange.[151] Google Marketing Platform contains the largest DSP, Display and Video 360, and the largest advertisers ad server in Campaign Manager 360.[152] Therefore, online platforms, and in particular Alphabet/Google and Meta/Facebook, remain the main beneficiaries of targeted advertising.[153]

III. TARGETED ADVERTISING AND CONSUMER PROTECTION LAW

Targeted advertising is a marketing strategy that is directed toward the consumers and, like all advertising, is a "commercial practice" regulated in the EU by the consumer protection rules.[154] These rules are designed to protect consumers' economic interests by

144. *See generally* Bennett Cyphers, *Don't Play in Google's Privacy Sandbox*, ELEC. FRONTIER FOUND. (Aug. 30, 2019), https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1 [https://perma.cc/T77T-A3WK] (archived Feb. 2, 2023).

145. *See* Kaifu Zhang & Zsolt Katona, *Contextual Advertising*, 31 MKTG. SCI. 980, 982 (2012).

146. *See* Veale & Borgesius, *supra* note 18, at 18.

147. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 6; *see also* EU Pol'y Report Online Advertising, *supra* note 19, at 38–39.

148. *See* COMPETITION & MKT. AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, APPENDIX M: INTERMEDIATION IN OPEN DISPLAY ADVERTISING M45–M46 (2020).

149. *See id*. at M31.

150. *See id*. at M12.

151. *See id*. (Google's Unified Action).

152. *Id.* at M71.

153. *See* CMA (UK) ONLINE PLATFORMS AND DIGITAL ADVERTISING STUDY, *supra* note 12, at 265.

154. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 2(d).

safeguarding consumer *autonomy* in the market,[155] which is characterized by asymmetries of power and significant potential for consumer harm.[156] As some practices of targeting advertising (e.g., behavioral advertising) are dependent on the processing of personal data, they are often discussed within the personal data protection and privacy frameworks in Europe. Landmark personal data protection legislation—the GDPR—was passed mainly as a response to the emergence of digital markets of personal data, for which behavioral advertising is a primary driver.[157] However, legislation that limits targeted advertising goes beyond personal data protection.[158] In this context, a particularly important body of law is consumer protection, which ensures that the practices of targeted advertising are fair to consumers in the European market, even when the personal data has been collected and used in a seemingly legally compliant manner.[159]

This Part elaborates on how the EU legal framework for consumer protection limits targeted advertising in four subparts. First, subpart A provides an overview of central consumer protection legislation; and describes how these provisions limit targeted advertising in two different stages. Second, subpart B addresses the contracting stage. Third, subpart C addresses the advertising stage. Lastly, subpart D elaborates on pending challenges of European consumer protection law.

---

155. *See* Michelle Everson & Crhsitian Joerges, *Consumer Citizenship in Postnational Constellations?* 5–7 (Eur. Univ. Inst., Working Paper No. 47, 2006); Marijn Sax, Between Empowerment and Manipulation 129 (2021) (Ph.D. dissertation, Universiteit van Amsterdam).

156. The legitimacy of legal doctrines of pre-World War II European nation-states was based on the principle of formal legal rationality that regarded a consumer as a sovereign party of a contract capable and expected to exercise full autonomy with regards to their contractual relationships. In post-World War II Europe, the rise of mass production resulted in a large-scale imbalance of bargaining power between traders (i.e., producers, sellers) and the consumers. Moreover, economic and physical harms demonstrated by the product scandals, for example, the drug thalidomide causing congenital disabilities in thousands of children around the globe, triggered a shift in legal doctrines for market intervention to regulate features of the imbalance of power and to protect consumers from potential harms. *See* DAVID BOLLIER & JOAN CLAYBROOK, FREEDOM FROM HARM 28–30 (1986); *see also* IRIS BENÖHR, EU CONSUMER LAW AND HUMAN RIGHTS 10–13 (2013).

157. The GDPR is in fact a further iteration and harmonization of data protection rules that were in existence since the 1990s. *See generally* General Data Protection Regulation, *supra* note 23; Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

158. Personal data protection legislation as well as safety legislation are sometimes considered to be part of larger consumer protection rules. However in practice is to differentiate privacy and safety protections for consumer protection as later is there to protect of consumers' economic interests. *See* TRZASKOWSKI, *supra* note 35, at 29–35.

159. *See* Natali Helberger, Frederik Zuiderveen Borgesius & Agustin Reyna, *supra* note 35, at 1427.

A. *EU Consumer Protection Law*

The foundation of EU consumer protection policies was laid out in Council Resolution 1975 O.J. (C 92)1,[160] which followed and was inspired by US President John F. Kennedy's formulation of consumer rights in the "Special Message to Congress on Protecting Consumer Interests" in 1962.[161] Since then, consumer protection has become one of the critical tasks of EU policy for the proper functioning of the internal market[162] and has been elevated as a fundamental rights objective.[163] Article 38 of the EU charter prescribes that EU policies "shall ensure a high level of consumer protection."[164] Note, however, that although a high level of consumer protection is mentioned in the Charter of Fundamental Rights of the EU, it is mentioned in the "solidarity" chapter within the list of rights that are usually referred to as "social" rights. Such rights also include, for example, the right to environmental protection.[165] While theoretically there is no hierarchy, in practice, the rights to personal data protection or privacy are generally easier to enforce as fundamental rights compared to the right to consumer protection that is still mostly aspirational.[166]

In EU secondary legislation, rules protecting consumers' economic interests, including those that concern targeted advertising, are spread amongst various pieces of consumer protection legislation. As already mentioned in the introduction, these are the Unfair Commercial Practices Directive (UCPD),[167] the Consumer Rights Directive (CPD),[168] the Unfair Contract Terms Directive (UCTD),[169] the Digital

---

160. 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.

161. John F. Kennedy, Special Message to the Congress on Protecting the Consumer Interest (March 15, 1962).

162. *See* Consolidated Version of the Treaty on the Functioning of the European Union arts. 12, 169(a), June 7, 2016, 2016 O.J. (C 202) 47 [hereinafter TFEU]. According to Article 12, "Consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities." *Id.* art. 12. According to Article 169(1), "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(a).

163. *See* Alan M. Sears, *The Limits of Online Price Discrimination in Europe*, 21 COLUM. SCI. & TECH. L. REV. 1, 19 (2020); Benöhr, *supra* note 156, at 14.

164. CFREU, *supra* note 21, art. 38.

165. *See* CFREU, *supra* note 21, art. 37.

166. *See* Helena U.Vrabec, Uncontrollable: Data Subject Rights and the Data-driven Economy (2019) (Ph.D. dissertation, Universiteit Leiden); Case C-470/12, Pohotovosť v. Miroslav Vašuta [2014] ECLI:EU:C:2014:101.

167. Unfair Commercial Practices Directive, *supra* note 37.

168. Consumer Rights Directive, *supra* note 38.

169. Unfair Contract Terms Directive, *supra* note 39.

Content Directive (DCD),[170] and most recently, the Digital Services Act (DSA).[171] As consumers are regarded as the weaker party in commercial dealings, such legislation aims to safeguard their autonomy and their economic interests by (i) empowering them with information ("information paradigm"),[172] and (ii) protecting them from unfair terms and practices ("unfairness paradigm").[173] The information paradigm permeates all of the consumer protection rules. In particular, extensive information requirements are provided within the CRD. The DSA introduces further transparency requirements that go beyond mere information disclosure.[174] Moreover, the UCTD, as well as the UCPD, have further information and sometimes transparency requirements. The information paradigm, embedded in European consumer protection legislation, is somewhat similar to the "transparency paradigm" of the GDPR.[175] It assumes that if consumers have enough information, they will exercise their autonomy by making informed decisions according to their individual goals, values, and preferences.[176] Consumer protection law has a benchmark of the "average consumer," which is considered to be a "reasonably well-informed and reasonably observant and circumspect" consumer that *understands* information and acts accordingly, for example, by accepting or refusing to enter the contract or use the services.[177]

While the information and now transparency paradigms permeate all consumer protection laws, the UCTD introduces rules for assessing unfairness for contractual terms, whereas the UCPD concerns the unfairness of commercial practices in general. The UCTD aims to protect consumers against unfair contract clauses.[178] Such terms may be present in standard form contracts, which comprise most (if not all) contracts for digital services.[179] In addition to addressing information asymmetry (stemming from the consumer being a weaker party), unclear terms must be interpreted in the most favorable way to the consumer (i.e., the rule of ambiguity in *dubio contra stipulatorem*).[180]

---

170. Digital Content Directive, *supra* note 40.

171. Digital Services Act, *supra* note 41.

172. *See* TRZASKOWSKI, *supra* note 35, at 270.

173. *See* Helberger, Borgesius & Reyna, *supra* note 35, at 9.

174. *See* Digital Services Act, *supra* note 41, arts. 15, 24, 27, 39, 42.

175. *See* Helberger, Borgesius & Reyna, *supra* note 35, at 9.

176. *See* TRZASKOWSKI, *supra* note 35, at 181.

177. *See* Case C-210/96, Gut Springenheide GmbH v Rudolf Tusky, 1998 E.C.R.I. I-4681, I-4691; *see also* Case C-371/20, Peek & Cloppenburg KG v. Peek & Cloppenburg KG, ECLI:EU:C:2021:674, ¶¶ 22, 41 (explaining 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").

178. *See* Unfair Contract Terms Directive, *supra* note 39, art. 1(1).

179. *See* 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.").

180. *See* Unfair Contract Terms Directive, *supra* note 39, art. 5.

The consumer has to infer meaning from individual contractual terms.[181] But some commentators have explained that fairness rules in contract law can also be used to include other societal policies or entitlements from fundamental rights in the assessment of fairness.[182]

The UCPD, in particular, is very important in a consumer protection toolbox, as it has a wider scope of application and acts as a safety net to all unfair practices whether or not such a method escapes the application of all other consumer protection legislation. The UCPD applies to business-to-consumer relationships and prohibits unfair commercial practices harming consumers' economic interests.[183] Article 5(2) of the UCPD lays out two cumulative requirements for practices to be regarded as unfair and therefore prohibited: "(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."[184]

While this is a general prohibition, the UCPD provides more specific provisions by which practices are prohibited. In particular, the UCPD further provides two more specific categories of unfair practices: those that are "misleading" and those that are "aggressive."[185] In determining whether a practice is misleading or aggressive, it must be determined whether that practice causes or is likely to cause the "average consumer" to make a transactional decision that he or she would not have otherwise made.[186] Furthermore, the UCPD contains a blacklist, where thirty-five practices are explicitly prohibited on the grounds that they are misleading or aggressive.[187]

To assess 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, consideration happens whether the practice is listed in Annex I as one of the *blacklisted practices*.[188] In such a case, no further consideration is necessary, and the practice is prohibited. Secondly, it must be assessed whether the

---

181. *See* TRZASKOWSKI, *supra* note 35, at 181.

182. *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).

183. *See* Unfair Commercial Practices Directive, *supra* note 37, arts. 3(1), 5(1), 1 (for business to consumer relationships, prohibition of unfair practices, and economic interests, respectively).

184. *Id*. 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).

185. *See id*. arts. 6–9.

186. *See*TRZASKOWSKI, *supra* note 35, at 181.

187. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 5, annex I.

188. *See id*. annex I.

practice is either "misleading" (through actions[189] or omissions[190]) and/or "aggressive,"[191] including when it exerts undue influence.[192] In case such misleading or aggressive practices have (or are likely to have) an economic effect as described above, they can be found unfair by ex post analysis and deemed prohibited. Lastly, the most general provision of the UCPD prohibits practices that are *otherwise* contrary to the requirements of "professional diligence."[193]

Requirements of information and unfairness paradigms apply to all advertising, including targeted advertising, that falls within the scope of "commercial practices" as defined by Article 2(d) of the UCPD.[194] Moreover, these provisions apply to targeted advertising not only during the advertising stage (when the personalized advertisement is displayed) but also when consumers provide their data to publishers (including online platforms) for targeted advertising purposes in exchange for receiving digital content or services (the contracting stage).[195] This Article further discusses the specific requirements in both stages of targeted advertisement.

B. *Contracts for Targeted Advertising?*

The Digital Content Directive (DCD) and the Digital Services Act (DSA) make the distinction between digital content and digital services.[196] While digital content refers to downloadable content, such as audio and video files, e-books, computer programs, and games (that are provided via a single act of supply), digital services entail the generally longer-term engagement of the consumer, often via subscriptions, and can include video and audio streaming, file hosting, and online gaming (including on social media).[197] In the context of the DCD and DSA, publishers of targeted advertising, as discussed in Part II, may be providers of digital content or services. A large amount of digital content and services that are accessed on websites or apps have

---

189. *Id*. art. 6.
190. *Id*. art. 7.
191. *Id*. art. 8.
192. *See id*. art. 9.
193. Otherwise, because misleading or aggressive practices are per se against professional diligence, therefore all blacklisted practices as well. *See id.* art. 5.
194. *Id*. art. 2(d).
195. *See generally* Digital Content Directive, *supra* note 40.
196. *See id*. art. 2(1)–(2); Digital Services Act, *supra* note 41.
197. *See* Digital Content Directive, *supra* note 40, art. 19. The actual distinction between digital content and digital services may be difficult to parse. Case C-641/19, EU v PE, 2020 E.C.L.I. 808 sheds more light on the boundaries. In cases of ambiguity, the practice in question will be regarded as a digital service (as this entails stronger protection for consumers). *See* 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, 2019) J. (L 328) 7 ¶ 30 [hereinafter Modernisation Directive].

been framed as "free," as consumers do not pay a monetary fee for accessing such services and are instead monetized by targeted advertising that utilizes the personal data of consumers accessing the website or the app.[198] Because of an assumption that economic exchange was absent, historically, the provision of such content and/or services was presumed to not be covered under consumer protection rules.[199] Nevertheless, over time, the consumer protection authorities of member states, such as those in Germany[200] and Italy,[201] have asserted that consumer protection rules apply in such cases, as consumers provide their monetizable attention and data in exchange for receiving content or services.

Following this rationale, the DCD has affirmed at the EU level that personal data can be considered as a counter-performance of a contract.[202] This provision contains an exception (i) for cases in which "the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service"[203] (including when *only* meta-data is processed),[204] or (ii) to allow "the trader to comply with legal requirements (e.g., the obligation to identify users).[205] Therefore, personal data would be the counter-performance where consumers access websites or apps that process the personal data of the consumer on any of the legal bases under data

198. This personal data is often combined with other, third-party sources of personal data for even more fine-grained targeting.

199. *See* Helberger, Borgesius & Reyna, *supra* note 35, at 3, 8.

200. 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.), https://bit.ly/3zQQaIW [https://perma.cc/394M-BNVH] (archived Feb. 20, 2023). 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.), https://bit.ly/3d4dQRm [https://perma.cc/9KWL-DYZT] (archived Mar. 28, 2023).

201. 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 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.), https://bit.ly/3OQWk06 [https://perma.cc/DWX6-ULQ9] (archived Feb. 20, 2023) [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), https://bit.ly/3oL0Sub (subscription required) [https://perma.cc/9QZ8-74M4] (archived Feb. 20, 2023).

202. *See* Digital Content Directive, *supra* note 40, art. 3.

203. *Id*. art. 3(1), ¶ 25.

204. *See 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.

205. Digital Content Directive, *supra* note 40, art. 3(1), ¶ 25.

protection law—other than contractual necessity or legal obligation.[206] This includes cases where consumers accept cookies on the basis of consent or publishers process personal data on the basis of legitimate interest, which in practice covers most publishers that monetize their business with targeted advertising.[207] There may be counterintuitively exceptional cases in which personal data may not be considered to be counter-performance where the actual service of a publisher is to provide consumers with personalized advertising,[208] as, for example, has been claimed in Meta's Terms of Service until April 5, 2023.[209]

The GDPR strengthened conditions for valid consent (e.g., informed, unambiguous, specific) for processing personal data that are typically not required for digital contracts.[210] On May 25, 2018, at midnight, when the GDPR came into force in the EU, Meta updated its terms and conditions, stating that it processed personal data because such processing was necessary to perform its core service, now framed as "personalization", seemingly bypassing the need for consumers' consent.[211] In July 2022, the European Data Protection Board decided in the *Meta Consent Bypass* case that such reframing was incompatible with the GDPR provisions regarding the legal basis used for processing personal data.[212] Following this decision, in December 2022, the Irish Data Protection Commission issued a €390 million fine for Meta.[213]

---

206. There are six legal bases upon which data controllers or processers can process personal data. These are detailed under Article 6(1) of the GDPR, and include (a) consent, (b) performance of a contract, (c) compliance with a legal obligation, (d) vital interests, (e) public interest, and (f) legitimate interests. General Data Protection Regulation, *supra* note 23, art. 6(1).

207. *See* IAB EUR. LEGAL COMM., GDPR GUIDANCE: LEGITIMATE INTERESTS ASSESSMENTS (LIA) FOR DIGITAL ADVERTISING 5 (Mar. 2021). [hereinafter Guidance on Consumer Rights Directive].

208. The wording of an exemption for Article 3(1) of the DCD is different from Article 6(1)(b) of the GDPR, which reads "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract." General Data Protection Regulation, *supra* note 23, art. 6(1)(b).

209. *See Terms of Service*, META (July 26, 2022), https://www.facebook.com/terms.php [https://perma.cc/ZC47-FBKQ] (archived Feb. 20, 2023); *How Meta Uses Legal Bases for Processing Ads in the EU,* META (Jan. 4, 2023), https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/ [https://perma.cc/9HZJ-SYHV] (archived Ap. 11, 2023).

210. *See* General Data Protection Regulation, *supra* note 23, art. 7. In many European jurisdictions consent for contracts can be implied. *See* CATERINA GARDINER, UNFAIR CONTRACT TERMS IN THE DIGITAL AGE 112 (2022).

211. *See BREAKING: Meta Prohibited from Use of Personal Data for Advertising,* NOYB (Jan. 4, 2023), https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising [https://perma.cc/7QP8-SE59] (archived Apr. 11, 2023).

212. *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).

213. *See generally* 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

Meta has announced to appeal the decision, and the case will likely reach the CJEU for final judgment.[214] However, to comply with this decision, it also updated its terms and conditions, and since April 5, 2023, it has relied on legitimate interest as a legal basis to serve personalized ads to users over the age of eighteen (it was already relying upon this legal basis to serve personalized ads for people under the age of eighteen).[215] In such cases, the DCD provision applies, and the personal data can be considered as counter-performance.

At first glance, treating personal data as a counter-performance comes in tension with data protection rules in two ways. Firstly, it can be interpreted as commodifying personal data that has fundamental rights protections in Europe,[216] and secondly, personal data protection rules require that consent for processing is not bundled with other terms.[217] However, the DCD recognizes both of these perspectives, stating that the GDPR has primacy in the context of data processing and acquiring consent,[218] clarifying that personal data is not a commodity and that the objective of the DCD is to empower consumers with contractual remedies.[219] The DCD places the consent requirements of the GDPR over its own provisions; therefore, the *freeness* of consent may depend on whether the publisher provides service if the consumer refuses data processing or at any time withdraws from it ("right to withdraw").[220] As a general presumption, the consent to provide personal data for targeted advertising purposes cannot be a condition for delivering digital content and/or services.[221]

In summary, in the context of targeted advertising, the DCD

Protection Regulation, Data Protection Commission (Dec. 31, 2022) (Ir.); In the matter of TSA, a complainant, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Instagram Service, Data Protection Commission (Dec. 31, 2022) (Ir.); 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, Data Protection Commission (Dec. 31, 2022). (Ir.)

214. *See Meta Advertising Ban – Decision Published*, NOYB (Jan. 23, 2023), https://noyb.eu/en/meta-advertising-ban-decision-published [https://perma.cc/3PFE-ZFZP] (archived Feb. 20, 2023).

215. *See How Meta Uses Legal Bases for Processing Ads in the EU,* META, *supra* note 209.

216. *See* Opinion 4/2017 of the European Data Protection Supervisor on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, at 3 (Mar. 14, 2017), https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf [https://perma.cc/VAU5-F962] (archived Mar. 28, 2023).

217. *See* General Data Protection Regulation, *supra* note 23, art. 7(2); *see also Planet49*, *supra* note 118, ¶ 58.

218. *See* Digital Content Directive, *supra* note 40, ¶ 24.

219. *See id.*

220. *See* General Data Protection Regulation, *supra* note 23, art.7(3).

221. *See id.* art. 7(4); *see also Guidelines 05/2020 of European Data Protection Board on consent under Regulation 2016/679*, v. 1.1. (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/UW26-F38U] (archived Mar. 28, 2023).

provisions complement the GDPR rules when it comes to the exchange of personal data for targeted advertising purposes. In cases where processing happens on a basis other than contractual necessity or legal obligation, such as when a consumer consents to personal data processing for targeted advertising (usually by accepting cookies), and such processing is valid under the GDPR (for example, if there is an option to refuse to target advertising cookies and have a service with lesser functionality), collected personal data will also be considered as counter-performance to a contract to which consumer protection rules apply. An interesting implication of regarding personal data as a counter-performance is, arguably, that contractual counter-performance may be taxed.[222] Nevertheless, it is yet unclear if any state will give such an interpretation (especially considering the disclaimer in the DCD that personal data is not a commodity).[223]

Another issue relates to the typical form of contracts that monetize digital content or services of targeted advertising publishers. Such contracts are generally either (i) *click-wrap* contracts that provide users with the notice of the terms of service and the possibility to accept them, or (ii) *modified click-wrap* contracts that provide users with an "accept" button and a hyperlink that takes them to the terms of service, or (iii) *browse-wrap* contracts that provide notice of terms as a hyperlink somewhere in the app or the website, agreement to which is implied by consumer accessing the digital content or the service (e.g., visiting a website).[224] While click-wrap contracts are generally considered valid and enforceable in most European jurisdictions,[225] the validity of modified click-wrap contracts and browse-wrap contracts is more controversial.[226] In contract law of all European jurisdictions, the

---

222. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 77.

223. *See* Digital Content Directive, *supra* note 40, ¶ 24.

224. *See* CATERINA GARDINER, UNFAIR CONTRACT TERMS IN THE DIGITAL AGE 105–7 (2022). The terminology of 'click-wrap' and 'browse-wrap' contracts comes from their predecessor—"shrinkwrap" license agreements for computer software. *See generally* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1293 (1995). In the 1990s, while software developers wanted to bind end-users by the terms of the contract, they were contracting the distributors, not the end-users. The solution to this was a shrinkwrap license, otherwise known as an "end user license agreement." Software was packaged in a plastic shrinkwrap that had terms printed on it. By purchasing such packaging, the end user was buying an option, not the software itself. Buy tearing the shrinkwrap end users were accepting the terms of service and entering into a contract with the software developers. "Click-wrap" agreements became a common practice when sales shifted towards the digital environment.

225. See, e.g., in France, *Association Famille de France v SA Père Noël.fr SA Voyage Père Noël.fr*, Tribunal de Grande Instance de Paris, 4 February 2003; in the Netherlands, *Netwise v NTS Computers*, Rechtbank Rotterdam, 5 December 2002, in *Computerrecht* 2003/02, 149; in Ireland, *Ryanair dac v SC Vola.ro srl* [2019] IEHC 239.

226. *See* MARCO B.M. LOOS, NATALI HELBERGER, LUCIE GUIBAULT, CHANTAL MAK, LODEWIJK PESSERS, KATALIN J. CSERES, BART VAN DER SLOOT & RONAN TIGNER, ANALYSIS OF THE APPLICABLE LEGAL FRAMEWORKS AND SUGGESTIONS FOR THE CONTOURS

"meeting of the minds" principle sets the fundamental requirements of voluntary acceptance of the terms of the contract.[227] The DCD, as well as the CRD, leaves the validity of the contracts to be assessed by national legislation.[228] Therefore, as the DCD's provision on data as counter-performance will apply only in cases where contracts are valid in the legislation of member states, some browse-wrap contracts and modified click-wrap contracts that provide consumers with digital content or services will remain outside of its scope. At first glance, this may suggest that, in such cases, consumer protection rules do not apply, but this is only the case to the extent of the direct application of the CRD. As shall be highlighted below, the UCPD has a wider scope and covers all commercial practices directed towards consumers, including when they are presented with browse-wrap contracts, as well as vague framing of digital services.

In cases where the contracts are considered valid, including when counter-performance of such contracts is personal data, the Consumer Rights Directive provides extensive information requirements.[229] Following the DCD's personal data as a counter-performance approach, the CRD requirements will apply in most cases when publishers monetize their content and/or services with targeted advertising (with a valid contract).[230] In general, in cases of "distance contracts" for digital content or services,[231] the CRD requires publishers to inform the consumer about, *inter alia*, the main characteristics of the service;[232] the publisher's identity and contact details;[233] the price,[234] functionality,[235] and interoperability of digital content,[236] which includes the fact that they will be tracked;[237] personalization taking place;[238] and the personalization of prices for content or services.[239]

OF A MODEL SYSTEM OF CONSUMER PROTECTION IN RELATION TO DIGITAL CONTENT CONTRACTS – FINAL REPORT, COMPARATIVE ANALYSIS, LAW & ECONOMICS ANALYSIS, ASSESSMENT AND DEVELOPMENT OF RECOMMENDATIONS FOR POSSIBLE FUTURE RULES ON DIGITAL CONTENT CONTRACTS 66–67 (2011).

227. *See* GARDINER, *supra* note 224, at 112.

228. *See* Digital Content Directive, *supra* note 40, art. 3(10), ¶ 12.

229. *See generally* Consumer Rights Directive, *supra* note 38.

230. *See* Consumer Rights Directive, *supra* note 38, art. 3(1); *see also* Guidance on Consumer Rights Directive, *supra* note 207, at 13–14.

231. The CRD refers to contracts concluded using distant means of communication—over the internet, including on online marketplaces, by telephone, etc. as "distance contracts." *See* Consumer Rights Directive, *supra* note 38, art. 2(7); *see also* Guidance on Consumer Rights Directive, *supra* note 207, at 8.

232. Consumer Rights Directive, *supra* note 38, art. 6(1)(a).

233. *Id.* art. 6(1)(b)–(d).

234. *Id.* art. 6(1)(e).

235. *Id.* art. 6(1)(r).

236. *Id.* art. 6(1)(s).

237. *Id.* ¶ 19.

238. Guidance on Consumer Rights Directive *supra* note 207, at 35.

239. *See* Consumer Rights Directive, *supra* note 38, art. 6(1)(e).

One of the cornerstones of consumer protection law is informing consumers about the total price of a contract.[240] Indeed, for the contracts of digital content and/or services, the CRD requires not only extensive information about all costs but also appropriate labeling of when the price is paid in exchange for the service or content ("buy now" instead of "confirm").[241] However, the DCD's definition of "price" as "money or a digital representation of value" seems to exclude from such requirements the contracts to which counter-performance is personal data.[242] Therefore, in cases when personal data is the counter-performance, the CRD does not include explicit and extensive requirements. Nevertheless, this is the third case in which the UCPD will apply.

Another cornerstone is informing consumers about the subject matter of the contract.[243] However, the validity of the contract, and therefore the correct framing of the main subject of the contract, is not itself covered by the CRD; instead, it includes requirements that information must be provided in a clear and comprehensible manner.[244] Such assessment is left for national courts to determine in individual cases (i) whether a given contract term relates to the definition of the main subject matter of the contract, or whether the examination of its unfairness would imply an assessment of the adequacy of the price and remuneration, and (ii) whether such contract terms are drafted in plain, intelligible language.[245] In contrast, further assessment of unfairness can be conducted under the UCPD regarding the subject matter and price, in that price indications may not be misleading.[246] In particular, the CJEU has previously emphasized that information about contract terms and the consequences of concluding a contract is of fundamental importance for a consumer and that "since the price is, in principle, a determining factor in the consumer's mind when it must make a transactional decision, it must be considered information necessary to enable the consumer to make such a fully informed decision."[247]

---

240. *See* Helberger, Borgesius & Reyna, *supra* note 35, at 10.

241. *See* Consumer Rights Directive, *supra* note 38, arts. 6(1)(c)–(d), 8(2); *see also* Guidance on Consumer Rights Directive *supra* note 207, at 44.

242. Digital Content Directive, *supra* note 40, art. 2(7); *see* Helberger, Borgesius, & Reyna, *supra* note 35, at 13. It seems that the DCD intentionally differentiates counter-performances of "price" and "personal data."

243. *See* Helberger, Borgesius & Reyna, *supra* note 35, at 10; Consumer Rights Directive, *supra* note 38, art. 6(1)(a).

244. *See* Unfair Contract Terms Directive, *supra* note 39, art. 4(2); *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) 4, 19 [hereinafter Guidance on the Unfair Contract Terms Directive].

245. *See* Case C-51/17 OTP Bank, OTP Faktoring v Teréz Ilyés, Emil Kiss, E.C.L.I. 750 ¶ 68 (2018); Case C-118/17 Zsuzanna Dunai v ERSTE Hank Hungery Zrt, E.C.L.I. 207 ¶ 49 (2019).

246. *See* Unfair Commercial Practices Directive, *supra* note 37, art. (6)(1)(d).

247. Case C-611/14, ECLI:EU:C:2016:800, ¶ 55 (2018).

Moreover, the Unfair Contracts Terms Directive (UCTD) excludes assessment of the fairness of a contract's price and subject, as long as the terms meet the transparency requirements.[248] Both the CRD and the UCTD leave the validity of contracts based on these two central issues to member states, given that they are conveyed in "plain, intelligible language."[249] This, therefore, leaves a gap as to how publishers (including online platforms) can frame the subject of the contract, or the main characteristics of their service, as well as what the consumer is giving in exchange for the service. No court has yet taken on the idea, which has permeated academic fields, that publishers should provide information about the monetary value they earn by processing the personal data of a particular consumer, or of a consumer on average.[250] People rarely know which data about them is captured, how those data will be used, and what the value is of those data.[251]

Nevertheless, as mentioned before, the UCPD has wider scope than both the CRD and UCTD and applies to all commercial practices directed toward consumers. This includes practices, such as browse-wrap agreements, framing the business of the social network as a personalization service, and information on the cost of the service when counter-performance of the service is personal data instead of the monetary price.[252] Firstly, blacklist item 20 in the blacklist of Annex I in the UCPD states that it is unlawful to describe a product as "gratis," "free," "without charge," or similar if the consumer must pay anything other than the unavoidable cost of responding to the commercial practices.[253] Italian courts have stated that Meta's slogan "it is free, and it is always going to be free" for their service to which consumers provide data for personalized advertising is not a free service and that Meta had to explain in detail how they monetize the services.[254] Nevertheless, it remains to be seen whether this principle will apply across the region. For example, while Google is very clear on the

248. *See* Unfair Contract Terms Directive, *supra* note 39, art. 4(2).

249. *Id*.

250. *See*, *e.g.*, Gianclaudio Malgieri & Bart Custers, *Pricing Privacy – The Right to Know the Value of Your Personal Data*, 34 COMPUT. L. & SEC. REV. 289, 290 (2018). A similar concept—being compensated for the use of one's personal data—was posited as early as 1995. *See* ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD 99–100 (1995).

251. The question remains of the remedies in case of such contracts, for example, to what extent is it possible to claim "economic damage" for consumers of "free" services.

252. *See* ePrivacy Directive, *supra* note 22, arts. 5(1), 6(1), ¶¶ 25–26; Digital Content Directive, *supra* note 40, ¶ 25.

253. Unfair Commercial Practices Directive, *supra* note 37, at 36.

254. *See* AGCM, *supra* note 201; *see also* Bianchi, *supra* note 201.

monetization of its products, they are still framed to be "free of charge" in its terms of service.[255]

The UCPD prohibits misleading actions, for example, the provision of false information, as well as misleading omissions, for example, not providing information that the UCPD deems "material" for the average consumer to make an informed transactional decision.[256] This encompasses all transactional decisions of consumers, which includes a decision to provide personal data for targeted advertising purposes.[257] As the Commission interprets the UCPD, even the action of scrolling through a feed and continuing to use the service can be considered a transactional decision.[258] In summary, for consumers that visit publishers' websites with modified click-wrap or browse-wrap contracts and make a transactional decision to continue using their services, the "material information" requirement of the UCPD is present, but what constitutes material is not explicitly defined.[259] In the context of targeted advertising, such material information may include specifying where more data is processed than necessary for the provision of the service, whether this data is monetized, and whether this data is used for personalization (including advertising, ranking, and pricing). If the trader does not inform a consumer that the data he is required to provide to the trader in order to access the service will be used for commercial purposes, this could be considered a misleading omission.

Moreover, the UCPD's unfairness test, in terms of "aggressive" practices, is directly applicable in the case when the publisher acquires consent from consumers via the cookie banners that can be regarded as "dark patterns" discussed earlier in Part II.B.[260] In these cases, it is not the amount of information and degree of transparency that determines the fair treatment of the consumer, but rather the way in which such information is displayed. Dark patterns, in this case, refer

---

255. *See Privacy and Security*, GOOGLE (Sept. 10, 2022), https://policies.google.com/?hl=nl [https://perma.cc/RD8S-L3KY] (archived Feb. 20, 2023). Meta's update took out "free" service. *See Terms of Service*, META (2023) https://www.facebook.com/legal/terms [https://perma.cc/AHD6-BFCH] (archived Feb. 20, 2023) ("We don't charge you to use Facebook or the other products and services covered by these Terms, unless we state otherwise. Instead, businesses, organizations, and other persons pay us to show you ads for their products and services. Our products and services enable you to connect with your friends and communities and to receive personalized content and ads that we think may be relevant to you and your interests. You acknowledge that by using our Products, we will show you ads that we think may be relevant to you and your interests. We use your personal data to help 834eterminee which personalized ads to show you.").

256. *See* Unfair Commercial Practices Directive, *supra* note 37, arts. 6–7.

257. *See 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*, O.J. 2021 (C 526) 1, 100 [hereinafter *Guidance on the Unfair Commercial Practices Directive*].

258. *See id*. at 99–101.

259. *See id*.

260. *See id*.

to malicious nudging generally incorporated into online interfaces.[261] Dark patterns do not have a legal definition in the UCPD. Instead, whether a specific pattern is prohibited under the UCPD will depend on the ex post case-by-case assessment of whether the material distortion to the consumers' decision-making is taking place.[262] In general, the UCPD is the central tool in the EU regulatory framework for handling "dark patterns"; however, it is complemented by other legal tools both within and outside consumer protection law.[263] For instance, when it comes to using dark patterns in order to acquire consent for processing personal data, the GDPR and ePrivacy Directive provisions take primacy, and therefore the provisions therein and those of the UCPD complement each other. In this context, the *Commission nationale de l'informatique et des libertés* (the French Data Protection Authority) fined Meta €60 millionand Google €150 million for not implementing an equivalent solution (button or other) that enables the user to refuse the placement of cookies equally easily.[264]

The Digital Services Act (DSA) introduces direct provisions prohibiting dark patterns, stating that "providers of online platforms shall not design, organize or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients of their service to make free and informed decisions."[265] This includes design choices of online platforms that may not be in consumers' best interest and is presented in the non-neutral manner, "such as giving more prominence to certain choices through visual, auditory, or other components."[266] Nevertheless, the DSA explicitly excludes practices that are already covered by the UCPD (business-to-consumer commercial practices) and the GDPR (practices involving personal data processing).[267] This can lead to an interpretation that the DSA does not prohibit dark patterns when consumers give consent to data processing for targeted advertising. Therefore, in such cases, the UCPD and the GDPR will apply in tandem to require publishers to devise online interfaces that grant the

---

261. *See id*.

262. Practices such as "continuous prompting," "privacy maze," "too many options," "skipping," or "deceptive snugness" have all been used to gather user consent. *See generally* Mark Leiser, *'Dark Patterns': the Case for Regulatory Pluralism, in* RESEARCH HANDBOOK ON EU DATA PROTECTION LAW 240 (Kosta et al. eds., 2021)

263. *See* EC STUDY ON DARK PATTERNS AND MANIPULATIVE PERSONALISATION, *supra* note 33, at 61–71.

264. *See Cookies: FACEBOOK IRELAND LIMITED Fined 60 Million Euros*, CNIL (Jan. 6, 2022), https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros [https://perma.cc/Q82Q-4DFK] (archived Feb. 20, 2023); *Cookies: GOOGLE Fined 150 Million Euros*, CNIL (Jan. 6, 2022), https://www.cnil.fr/en/cookies-google-fined-150-million-euros [https://perma.cc/T6CY-54L4] (archived Mar. 14, 2023).

265. *See* Digital Services Act, *supra* note 41, art. 25(1)(a).

266. *Id.* ¶ 67.

267. *See id.* ¶ 10.

same level of protection as the DSA and that present a neutral choice when requesting consumers to "accept" or "reject" such data processing.

Moreover, one of the significant provisions for consumer protection found its way into the Digital Markets Act that sets additional rules from a competition law perspective, in particular, the gatekeeper online platforms when they also act as advertising networks and collect their consumers' personal data from third-party publishers.[268] With the aim in mind to neutralize some of the network effects, the DMA requires gatekeepers[269] to provide their "core services" with the less personalized alternative, not making the provision of their services conditional to the consumers' consent.[270] Moreover, gatekeepers are not allowed to combine personal data sourced from these core platform services with personal data from any other services offered by them or with personal data from third-party services unless the end-user has been presented with the specific choice (e.g., between Google Maps and Google Search, or between Facebook and Instagram).[271] This can significantly limit targeted advertising which draws on data from multiple sources.[272]

C. *Personalizing Advertisements to Consumers*

The content of advertisements presented in the EU is heavily regulated. For example, the Audiovisual Media Services Directive sets requirements for advertisements in audiovisual media services that, in the context of the digital world, include video-on-demand (e.g., YouTube orNetflix), as well as social media platforms that allow video sharing (e.g., TikTok or Instagram).[273] Online platforms are required to protect the general public from content that promotes hate speech, terrorism, child pornography, racism, and xenophobia.[274] Moreover, the Audiovisual Media Services Directive requires advertisements to be recognizable, not to use subliminal techniques, and sets other

---

268. *See* Digital Markets Act, *supra* note 28, ¶ 36.

269. A gatekeeper is defined on the basis of a cumulative three criteria test, namely: (i) significant impact on the EU internal market; (ii) control of an important gateway for business users to reach end-users; and (iii) entrenched and durable position. *See id.* art. 3(1), ¶ 36.

270. *See id*. ¶ 37 ("At the time of giving consent, and only where applicable, the end user should be informed that not giving consent can lead to a less personalised offer, but that otherwise the core platform service will remain unchanged and that no functionalities will be suppressed.").

271. *See id*. ¶ 36.

272. *See* SARTOR & GALLI, *supra* note 35, at 30.

273. *See* 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) art. 1(a)(i)–(ii), (g) [hereinafter Audiovisual Media Services Directive].

274. *See id.* art. 27, ¶ 1.

content restrictions (e.g., for tobacco and alcohol products).[275] Apart from the Audiovisual Media Services Directive, rules regarding copyright, counterfeit goods, trademarks, as well as certain goods such as financial, gambling, alcohol, or pharmaceuticals create a plethora of prohibitions and restrictions for the content of targeted advertising.[276]

The Digital Services Act (DSA) is a holistic online platform regulation by setting new standards for accountability across online platforms regarding illegal and harmful content.[277] Moreover, with an intention to protect consumers online, the DSA directly regulates targeted advertising by setting rules not only for the content of the advertisements but also for their targeting.[278] It recognizes the risks associated with personalization, such as manipulation and discrimination, and imposes transparency requirements for targeted advertisements online.[279] Firstly, as in the Audiovisual Media Services Directive, online platforms are required to ensure that consumers can identify the communication they see as an advertisement.[280] This must be ensured in a way that is unambiguous for the "average consumer" and may include standardized visual or audio marks.[281] Secondly, online platforms are required to inform consumers about who the "advertiser" is—that is, a natural or legal person who pays for placing the advertisement.[282] Moreover, platforms are also required to disclose on whose behalf the advertisement is presented when this is different from the advertiser (e.g., advertising networks or SSPs).[283] Lastly, the DSA requires platforms to provide "meaningful information" about the main parameters used for targeting and, where it is feasible, allow consumers to change those parameters.[284] This transparency requirement is aimed at helping users to oppose targeted advertising by refusing to be profiled on data protection grounds.[285]

The Digital Services Act enacts additional targeted advertising transparency rules for *very large online platforms* (also very large search engines) that provide their services to more than 45 million

---

275. *See id*. arts. 9(b), 11(4).

276. *See Advertising Policies*, META, https://www.facebook.com/policies_center/ads (last visited Feb. 10, 2023) [https://perma.cc/M83C-FSUN] (archived Feb. 10, 2023); *see also Google Ads Policies*, GOOGLE, https://support.google.com/adspolicy/answer/6008942?hl=en (last visited Feb. 10, 2023) [https://perma.cc/LFP5-NHYF] (archived Feb. 10, 2023).

277. *See* European Commission Press Release IP/10/63, Europeans' Privacy Will be big challenge in next decade, says EU Commissioner (Jan. 28, 2010).

278. *See* Digital Services Act, *supra* note 41, ¶ 68.

279. *See id*. ¶ 94.

280. *See id*. art. 26, ¶ 1(a).

281. *See id.* art. 35, ¶ 69 (the DSA promotes the development of voluntary standardizations for advertising).

282. *See id*. art. 26(c).

283. *See id*. art. 26(b).

284. *See id*. art. 26(d).

285. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 88–89.

average monthly active recipients.[286] The DSA requires very large online platforms to make an available repository of the content of the advertisements through their application programming interfaces.[287] Such a repository must contain information about the advertisers for each campaign,[288] the person or the organization that paid for displaying the advertisement when different from the advertiser (e.g., an ad network or SSP),[289] the consumer audience(s) to whom the advertisement was targeted and the main parameters used for that purpose,[290] and the total number of consumers reached in each member state.[291]

In addition to transparency obligations, the Digital Service Act contains two general prohibitions with regard to targeted advertising practices. These prohibitions stem from the premise that in these specific instances, risks of targeted advertising that profiles people based on their interests (i.e., behavioral advertising) can potentially exploit consumer vulnerabilities and result in their manipulation are particularly high.[292] Firstly, the DSA prohibits targeted advertising based on profiling when platforms are "aware with reasonable certainty" that the consumer is a minor.[293] The DSA further explains that this prohibition should not lead online platforms to obtain more information in order to identify that the consumer is a minor.[294] Secondly, the DSA prohibits targeted advertising based on profiling using special categories of data.[295] Therefore, for behavioral-advertising purposes, consumers cannot be segmented into the categories of sexual orientation, political affiliation, race, or health condition.[296]

The central issue with regards to the prohibition of behavioral advertising based on special categories of data is the breadth of interpretation of personal data and whether it includes inferences, predictions, and assumptions that refer to or impact an individual.[297] In behavioral advertising, some attributes are inferred algorithmically. Such inferences can directly relate to protected attributes (e.g., interest in the LGBTQ community); in this case, inferences are treated no differently than special categories of data voluntarily disclosed by the

---

286. *See* Digital Services Act, *supra* note 41, art. 33, ¶ 1.
287. *See id*. art. 39, ¶ 1.
288. *See id*. art. 39, ¶ 2.
289. *See id*.
290. *See id*.
291. *See id*.
292. *See id*. ¶ 69.
293. *Id*. ¶ 71.
294. *See id*.
295. *See id*.; General Data Protection Regulation, *supra* note 23, art. 9, ¶ 1.
296. *See* Digital Services Act, *supra* note 41, ¶ 69.
297. *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 498 (2019).

consumers and, therefore, are prohibited by the DSA.[298] In practice, online platforms already limit behavioral advertising based on special categories of data. Already in 2021, Meta announced the removal of "detailed targeting" options that relate to topics people might perceive as sensitive, such as categories related to health, race or ethnicity, political affiliation, religion, or sexual orientation.[299] Similarly, Google's personalized advertising policies restrict targeting advertising based on sensitive categories of data, including when for example, consumers are particularly vulnerable (e.g., going through a divorce, health concerns, etc.).[300] However, what is covered by the special categories of data can be interpreted more broadly and include the source data from which sensitive inferences can be drawn (e.g., postcode, last name, or location of birth to infer race or ethnic origin).[301] In August 2022, the CJEU issued preliminary ruling C-184/20, which supports this position.[302] This judgment has significant consequences for behavioral advertising as, arguably, AI systems can infer sensitive information from a variety of data processed by the publishers (e.g., sexual orientation based on browsing history). While further guidance is needed to see under what conditions (e.g., intentionality or reliability) source data can be classified as proxy and, therefore, special categories of data,[303] there is a chance that the C-184/20 judgment, together with the DSA prohibition, may act as the *de facto* ban on behavioral advertising.

Banning behavioral advertising as such has been proposed before by the media and civil society.[304] European Parliament has also called for prohibiting "micro-targeting,"[305] and the European Data Protection Supervisor has proposed a phase-out prohibition of targeted advertising on the basis of "pervasive tracking."[306] The prohibition in

---

298. *See id*. at 569.

299. *See Removing Certain Ad Targeting Options and Expanding Our Ad Controls*, META (Nov. 9, 2021), https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls [https://perma.cc/G8LT-2J3C] (archived Feb. 10, 2023).

300. *See Personalized Advertising*, GOOGLE, https://support.google.com/adspolicy/answer/143465#250 (last visited Feb. 10, 2023) [https://perma.cc/G9HE-V9QK] (archived Feb. 10, 2023).

301. *See* Wachter & Mittelstadt, *supra* note 299, at 78.

302. *See* Case C-184/20, OT v. Vyriausioji Tarnybinės Etikos Komisija, ECLI: EU:C:2022:601, ¶ 123 (Aug. 1, 2022).

303. *See* Wachter & Mittelstadt, *supra* note 299, at 73–77.

304. *See, e.g.*, Gilad Edelman, *Why Don't We Just Ban Targeted Advertising?*, WIRED (Mar. 22, 2020, 7:00 AM), https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/ [https://perma.cc/N9KU-HZDX] (archived Feb. 10, 2023); *Coalition Letter*, BAN SURVEILLANCE ADVERT., https://www.bansurveillanceadvertising.com/coalition-letter (last visited Feb. 11, 2023) [https://perma.cc/BR6A-4UHB] (archived Feb. 10, 2023); FORBRUKERRADET, TIME TO BAN SURVEILLANCE ADVERTISING (2021).

305. *See* European Parliament Resolution of 18 June 2020 on Competition Policy, 2021 O.J. (C 362) 22, 35 ¶ 105.

306. *See* WOJCIECH WIEWIORÓWSKI, OPINION 1/2021 ON THE PROPOSAL FOR A DIGITAL SERVICES ACT 3 (Feb. 10, 2017).

the PAIA of *subliminal*[307] or *manipulative* AI that "materially distorts behavior"[308] can also be interpreted as indirectly banning behavioral advertising to the extent to which it relies on AI.[309] The rationale for such broader prohibitions is that behavioral advertising may exploit consumers' decision-making vulnerabilities, manipulating them into economic decisions that are against their best interests.[310] From the economic perspective, such harmful outcomes can be, for example, consumers buying something they would not buy otherwise or paying more than they would if they had not been exposed to such an advertisement.[311] Moreover, manipulation also harms consumers by stripping them of their agency which can further result in physical or psychological harm.[312]

Concerns about consumer manipulation stem from insights into human decision-making, revealing that consumers don't usually make entirely rational decisions but base their choices on heuristics (shortcuts) and biases, sometimes cumulatively referred to as decision-making *imperfections* or *vulnerabilities*.[313] While market players have always had an incentive, and have actively tried, to exploit such imperfections of decision-making,[314] online platforms have an unprecedented position that gives them not only the visibility of such vulnerabilities through real-time observation of human behavior but also *personalizing* the decision-making environment in real-time,[315]

---

307. *See* Proposal Artificial Intelligence Act, *supra* note 30, art. 5, ¶ 1(a) (prohibiting "the placing on the market [and] putting into putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm").

308. *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").

309. For both prohibitions, the reference made to consumer protection law, in particular in the UCPD, is evident not only because of the reference to "material distortion of behavior" but also dimensions of vulnerability and manipulation. *See* GALLI, *supra* note 35, at 264–65.

310. *See* Calo, *supra* note 34, at 1033 ("In its purest form, digital market manipulation recognizes that vulnerability is contextual and a matter of degree and specifically aims to render all consumers as vulnerable as possible at the time of purchase.") .

311. *See* Susser, Roessler & Nissenbaum, *supra* note 34, at 26–29.

312. *See* GALLI, *supra* note 35, at 265.

313. *See generally* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2012); ROBERT B. CIALDINI, INFLUENCE: THE PSYCHOLOGY OF PERSUASION (2007); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE (2021).

314. *See* Jon D. Hanson and Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation* 74 N.Y.U. L. REV. 630, 721–44 (2008).

315. Karen Yeung describes the problem in terms of "hypernudging." *See* Karen Yeung, '*Hypernudge:' Big Data as a Mode of Regulation by Design*, 20 INFO. COMM. & SOC'Y 118, 119 (2017).

making it possible to personalize advertisement in a way that catches consumers in the moment in time when they are most vulnerable.[316]

While the concerns about consumer manipulation are not new, assessing whether manipulation actually happens is more complicated.[317] Some studies conclude that manipulative personalization is prevalent in targeted advertising,[318] while others suggest that targeting can have no effects or sometimes even positive effects for the consumer.[319] Its plausible that due to such perceived uncertainty about the actual negative impacts of behavioral advertising, the Commission found it disproportional to outright ban the practice (at least explicitly), which is the primary revenue stream for some of the largest companies and generates a massive amount of wealth in the EU. Instead, the DSA's transparency provisions, particularly for advertising repositories for very large online platforms, are intended to shed more light on how targeting happens so that researchers and policymakers can assess the extent to which targeted advertising practices of online platforms exploit human vulnerabilities.[320] Note that the DMA echoed similar and more stringent requirements, including empowering the Commission to gain access to data and algorithms of "gatekeepers."[321]

Regardless of the breadth of interpretation of DSA prohibitions, the UCPD provides a final filter for assessing the legitimacy of targeted advertising practices, including when it concerns manipulative influence. Commercial practices can violate the UCPD in five different ways: being on a blacklist, a misleading omission, a misleading action, an aggressive action, or failing the general test.[322] As the UCPD is a maximum harmonization directive, member states cannot add prohibited practices themselves to the list.[323] However, if EU legislators regard any specific targeted advertising practice as unfair, the UCPD would be the most apt location to proscribe it. For example, item 11 of Annex I prohibits providing search results without clearly disclosing any paid advertisement or payment specifically for achieving a higher ranking of products within the search results.[324]

---

316. *See* Susser, Roessler & Nissenbaum, *supra* note 34, at 38–40; *see also* Calo, *supra* note 34, at 1031.

317. *See* Susser, Roessler & Nissenbaum, *supra* note 34, at 12–29.

318. *See* EC STUDY ON DARK PATTERNS AND MANIPULATIVE PERSONALISATION, *supra* note 33, at 59–60.

319. *See* 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. 719, 725–26 (2019).

320. *See* Digital Services Act, *supra* note 41, ¶ 95.

321. *See* Digital Markets Act, *supra* note 28, art. 21.

322. *See* Laux, Wachter & Mittelstadt, *supra* note 319, at 744. Under the proposed DMA, gatekeeper platforms would have to submit to the Commission an independently audited description of any consumer profiling techniques they use. Digital Markets Act, *supra* note 28, art. 15.

323. *See* EU Pol'y Report Online Advertising, *supra* note 19, at 70.

324. *See* Unfair Commercial Practices Directive, *supra* note 37, annex I, ¶ 11.

Similarly, the EU legislators may consider reiterating the DSA, DMA, and PAIA prohibitions on the blacklist of the UCPD.

Further, the UCPD prohibits the *misleading omission* of material information that consumers need to have for making transactional decisions (that under the UCPD includes scrolling the feed, as well as clicking the advertisement).[325] In this context, the DSA transparency requirements for online platforms regarding targeting criteria can be considered for the UCPD as such material information. However, these requirements would not apply for non-platform publishers unless they commit to them through voluntary codes of conduct.[326] Further explicit guidance from the Commission or the decisions of national authorities and courts may shed light on the ambiguity of what constitutes material information non-platform publishers must inform their consumers about when presenting personalized advertising. However, it is highly likely that such material information will be interpreted as similar to the requirements of online platforms and, at minimum, require all publishers to inform consumers that the advertisement is personalized, as well as targeting criteria.

Prior to the DSA, a similar provision requiring consumers to be informed about the main parameters of algorithmic decision-making (not the algorithms themselves) was introduced by the Directive (EU) 2019/2161 on Enforcement and Modernisation in relation to *ranking offers* that mainly refer to search results but also apply cases of paid ranking that are a form of targeted advertising (*see* Part II.B.).[327] Firstly, for online search engines (and online platforms more broadly), ranking transparency rules were introduced by the Regulation (EU) 2019/1150 (Platform to Business Regulation—P2B),[328] that primarily sets out extensive obligations for online platforms to inform their business users about the ranking criteria (that in case of paid ranking would involve advertisers, ad intermediaries, or publishers).[329] Such transparency rules were also reflected in the CRD as an obligation of online marketplaces to disclose the main criteria for ranking, this time

---

325. *See id*. art. 7.

326. *See* GALLI, *supra* note 35, at 267.

327. *See* Modernisation Directive, *supra* note 199, ¶¶ 18–23; *see also* EU Pol'y Report Online Advertising, *supra* note 19, at 61; *supra* Part II.B.

328. 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].

329. P2B Regulation addresses power asymmetries between online platforms and smaller businesses, including in the context of paid ranking (form of targeted advertising), other publishers, ad intermediaries, and advertisers. It requires online platforms to be transparent about how ranking is conducted in terms and conditions directed towards their business customers, including information about if ranking parameters are against any direct or indirect payment, as well as if personalization of the ranking takes place, and if it is based on consumers' search behavior, interests, geographic location, time of day search takes place, etc. *See* Guidance on Ranking Transparency, *supra* note 66.

for consumers.[330] In the same vein, the UCPD considers the main parameters of ranking as material information that should be conveyed to consumers by all publishers providing such ranking.[331] Information requirements in the CRD and UCPD are less detailed than under P2B, with an intention to be more concise and easily understandable, and they include main parameters of ranking, weights the parameters are given, and how (if) they are monetized.[332]

Lastly, the CRD requires the provision of additional information when the offered price is personalized based on automated decision-making.[333] However, this requirement is for "before the consumer is bound by a distance contract," therefore likely relating to a purchasing decision rather than any transactional decision—for example, clicking the advertisement that includes price personalization.[334] Nevertheless, not including information that the prices in targeted advertising are personalized would most likely constitute a misleading omission under the UCPD, as personalized prices are covered by the UCPD beyond purchasing decisions.[335]

Any active deception in disclosed information will constitute *misleading action* that the UCPD also prohibits.[336] In the context of targeted advertising, this can be, for example, an online platform disclosing false targeting criteria. While provisions on misleading omission and action are necessary, they are not sufficient for assessing the fairness of targeted advertising practices. Instead, targeting criteria and logic involved (whether disclosed or not) can be unfair when it becomes *aggressive* by exerting undue influence.[337] Such undue influence can be argued to come from the informational and technical power of publishers (whether online platforms or other publishers that also use advertising networks or other ad intermediaries) coupled with the exploitation of misfortunes (circumstances of gravity). For example, suppose it is disclosed that the targeting criteria are the consumer's health status or political views, or being divorced. In that case, such influence can be regarded as aggressive under the UCPD,[338] in the vein of the DSA prohibition of

330. *See* Consumer Rights Directive, *supra* note 38, art. 6, ¶ 1(a).

331. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 7, ¶ 4(a).

332. *See generally* Guidance on Ranking Transparency, *supra* note 66.

333. *See* Consumer Rights Directive, *supra* note 38, art. 6, ¶ 1(e).

334. *Commission Proposal for a Directive of the European Parliament and of the Council Amending Directive 2011/83/EU Concerning Financial Services Contracts Concluded at a Distance and Repealing Directive 2002/65/EC*, ch. IIIa art. 16a(1), COM (2022) 204 final (May 11, 2022); EU Pol'y Report Online Advertising, *supra* note 19, at 63.

335. *See* Sears, *supra* note 31, at 21. *See* Guidance on the Unfair Contract Terms Directive, *supra* note 244, § 3.4.6 ("[T]he possible unfairness of a contract term can be closely related to its lack of transparency or the lack of transparency of a contract term may even indicate its unfairness.").

336. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 6.

337. *See* GALLI, *supra* note 35, at 234.

338. *See* GALLI, *supra* note 35, at 238–40.

targeting based on data that is sensitive. As discussed above in this subpart, through a broad interpretation of the DSA prohibitions coupled with the C-184/20 judgment on sensitive inferences,[339] there is the chance that behavioral advertising, in its entirety, comes under scrutiny as an aggressive practice. This is because there is not an obvious way to guarantee that the targeting criteria of search history or browsing history that are further usually analyzed by black-box algorithms do not process sensitive criteria (e.g., health, political views) in their intermediate functioning.[340]

Nevertheless, suppose behavioral advertising practice escapes the DSA prohibitions and C-184/20 judgment. In that case, courts will have to assess ex post in each particular advertising practice how likely it is that the targeted consumers are seeing advertisements that are trying to exploit vulnerabilities.[341] As an example, Meta's earlier adoption of a transparency mechanism of targeting criteria revealed that in Denmark, payday loans were targeted at people with interest in gambling.[342] This was found "unfair" by the Danish consumer ombudsman.[343] Beyond aggressive practices, the fifth way to assess the fairness of targeted advertising practices is the general unfairness test of the UCPD, which prohibits practices that materially distort consumer behavior and are contrary to professional diligence.[344] Arguably, the criteria of "'honest market practices" and "general principle of good faith" in this requirement "leaves room for normative judgment."[345] Meeting the requirements of the GDPR and ePrivacy Directive can be seen as part of professional diligence.[346] In practice, particularly important may be publishers' reliance on Interactive Advertising Bureau Europe's TCF that combined the consumer consent across the internet, the case that now reached the CJEU with the request for the preliminary ruling.[347]

It seems that ex post analysis of whether certain targeted advertising practices are *aggressive* or *against professional diligence* in that they distort consumer behavior by exploiting consumer vulnerabilities will be prominent in the years following the DSA's coming into force.[348] Nevertheless, in consumer protection law, not all behavioral exploitation is a failure of the market that requires correction (for example, *puffery*—or boastful exaggeration—is

339. *See* Case C-184/20, *supra* note 304, ¶ 123.
340. *See* GALLI, *supra* note 35, at 234.
341. *See* Laux, Wachter & Mittelstadt, *supra* note 319, at 744.
342. *See* TRZASKOWSKI, *supra* note 35, at 246.
343. *Id.* at 246.
344. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 5, ¶ 2.
345. GALLI, *supra* note 35, at 248.
346. *See* Philip Hacker, *Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law*, EUR. L.J. 1, 12 (2021).
347. *See IAB Europe case: The Market Court refers preliminary questions to the Court of Justice of the EU*, *supra* note 142.
348. *See* GALLI, *supra* note 35, at 248.

considered fair play in advertising).[349] This is because the European regulator chose not to overregulate in cases when the impacts of commercial practices are negligible.[350] Rather, in order for the practices to be unfair, they have to be exploitative for the "average consumer."[351] In the context of targeted advertising, the benchmark is the "average targeted consumer"—or the average member of that targeted audience.[352] If, for example, an advertisement is targeted to women, between the ages of twenty-five and thirty-five, with an expressed interest in financial products, the unfairness of the practice (that is the extent to which the practice is against professional diligence, misleading, or aggressive) must be assessed from the perspective of the "average" member of the group. In this case, an adult interested in financial products will be expected to deliberate and form judgments as to the advertisement.

The UCPD provides further protection for "targeted vulnerable consumers" that are vulnerable because of their characteristics, such as mental or physical infirmity, age, or credulity.[353] In cases when advertising is targeted to such consumers, whether consumer behavior is likely to be distorted must be assessed from the perspective of the average member of such a group of vulnerable consumers. More recent interpretations of the Commission on *consumer vulnerability* take into account situational and dynamic vulnerabilities that are universal to all human beings (beyond mental, physical infirmity, age, etc.).[354] With this interpretation, targeting advertisements for payday loans to people with a gambling addiction will be assessed from the perspective of a person addicted to gambling. However, the missing piece in UCPD enforcement is the notion of "digital vulnerability"—that is, the understanding of consumers as universally vulnerable in digital environments.[355] Many in academia have argued that the power asymmetries present (especially between online platforms and consumers) in targeted advertising, as well as in immersive digital environments, require recognition of the consumers as being universally vulnerable in digital environments.[356] The UCPD is

---

349. *See* Laux, Wachter & Mittelstadt, *supra* note 319, at 740.

350. *See* Unfair Commercial Practices Directive, *supra* note 37, ¶ 6.

351. *See* Cristopher Decker, *Concepts of the Consumer in Competition, Regulatory, and Consumer Protection Policies*, 13 J. COMPETITION L. & ECON. 151, 184 (2017).

352. Unfair Commercial Practices Directive, *supra* note 37, ¶ 18.

353. Unfair Commercial Practices Directive, *supra* note 37, art. 5, ¶ 3.

354. *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 [https://perma.cc/KAD4-CBVD] (archived Feb. 12, 2023).

355. *See* GALLI, *supra* note 35, at 181–205.

356. *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); Laux,

flexible enough for national authorities and the CJEU to interpret consumers in the digital environment as vulnerable in the context of targeted advertising. Nevertheless, with immersive technologies (i.e., the Metaverse) on the horizon, proactive clarification of the European legislator on the consumer benchmark can positively impact European consumers' experiences in digital environments.

This Article further discusses the central challenges the consumer protection law faces in the context of targeted advertising, including digital vulnerability, challenges with the enforcement, remedies, and considerations of market power when it comes to targeted advertising.

D. *Targeted Advertising and the Fitness Check of Consumer Protection Law*

In 2022, the Commission announced a "fitness check" of EU consumer protection law that will analyze whether additional action is needed to ensure an equal level of fairness in offline and digital environments.[357] In particular, the Commission will evaluate the rules of the UCPD, UCTD, and CRD.[358] The fitness check must take into consideration targeted advertising, which is one of the primary features of the consumers' digital experience. In this context, existent rules of analyzed directives will apply together with ex ante rules of the DSA, DMA, and PAIA, which will improve consumers' normative position in targeted advertising.[359] The analysis must also take into consideration the application of consumer protection rules with the GDPR and ePrivacy Directive, as only through such a holistic overview of rules from competition, personal data protection, and consumer protection law can it successfully neutralize some of the harms of targeted advertising.

The remaining issues that the Commission must consider in regards to increasing the fairness of digital environments are (i) evolving the information paradigm into a "transparency paradigm," (ii) updating the rules for standard contractual terms in the digital environment, (iii) requiring publishers to disclose the monetary value of monetized data (similar to price disclosure requirements), (iv) providing further guidance on online interface design, (v) updating the UCPD's blacklist to define the limits of targeted advertising, (vi)

Wachter & Mittelstadt, *supra* note 319; GALLI, *supra* note 35, at 188–92; TRZASKOWSKI, *supra* note 35 at 115-120; NATALI HELBERGER, ORLA LYNSKEY, HANS-WOLFGANG MICKLITZ, PETER ROTT, MARIJN SAX & JOANNA STRYCHARZ, EU CONSUMER PROTECTION 2.0, STRUCTURAL ASYMMETRIES IN DIGITAL CONSUMER MARKETS, BEUC at Part I (2021).

357. *See Digital Fariness – Fitness Check on EU Consumer Law*, EUR. COMM'N (Sept. 10, 2022), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en [https://perma.cc/53K7-ANRC] (archived Feb. 12, 2023).

358. *See id*.

359. *See* Laux, Wachter & Mittelstadt, *supra* note 319, at 748; *see also* GALLI, *supra* note 35, at 266–69.

revisiting concepts of consumer vulnerability in digital environments, and (vii) updating rules to enable cross-border collective actions.

Firstly, the information paradigm is somewhat limited in the online world. Consumers have limited cognition and resources (e.g., time and attention), and enriching them with information may disempower them.[360] Online, the most efficient strategy often is to ignore the information to avoid information overload.[361] Information disclosure can, in a way, be used to push people towards avoiding being informed, manipulating them away from their best interests.[362] In order for consumer rights (e.g., the right to withdraw under the CRD) to be an effective tool, consumers must be aware of and ready to pursue their rights.[363] Therefore, anything less than a transparency paradigm—that ensures the provision of information in a way that appeals to consumers' capacity for reflection and deliberation—in the digital world will be futile in consumer empowerment.[364] Transparency would mean using images, videos, audio, or textual means such as framing effects, to level information asymmetries.[365] In practice, often, the opposite is the case, and information is framed in a way that poses privacy risks in a positive way.[366] One example of such framing is Meta's description of its primary service as a "personalization service."[367] Consumer protection rules in the CRD, UCTD, and UCPD must be updated to meet the transparency paradigm, similar to rules in the DSA, DMA, and GDPR.

Secondly, limitations of the information paradigm and loss of consumer choice are most visible when consumers are contracting publishers of digital services and content. The digital environment cannot continue to function on click-wrap and browse-wrap contracts that leave consumers without an actual choice.[368] While such rules are traditionally withheld at the EU in accordance with the principle of autonomy of the member states in contractual matters,[369] the cross-border nature of these contracts and collective harms stemming from them require EU-level intervention. One option would be introducing rules and standardizing contractual clauses for distance contracts that would act as the default mode for consumers in the digital environment.[370] In such an online environment, publishers could introduce their preferred alternative terms, but only when they clearly

---

360. *See* TRZASKOWSKI, *supra* note 35, at 195–97.

361. *See id*.

362. *See generally* Hao Wang, *Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency*, 35(69) PHIL. & TECH. 19 (2022).

363. *See* Consumer Rights Directive, *supra* note 38, art. 6, ¶ 1.

364. *See* TRZASKOWSKI, *supra* note 35, at 196.

365. *See id*. at 185.

366. *See id*. at 186.

367. *See Terms of Service*, META, *supra* note 209.

368. *See generally* Gardiner, *supra* note 224.

369. *See* Gardiner, *supra* note 224, at 136.

370. *See generally* Lemley, *supra* note 224.

communicate to each consumer deviation from standardized clauses to which consumers would have to explicitly assent, transforming digital contracts into having an actual benefit of the bargain where a consumer can express their choice.[371] These standardized rules are relevant for targeted advertising, as they may include the requirement to provide a less-personalized alternative of digital services and content as a default end to enable personalized alternatives only when a consumer explicitly opts in for this.[372] A similar requirement is echoed in the DMA for gatekeeper platforms that provide "core platforms services" such as search engines or social networking.[373] As sunk costs and network effects add friction to consumers' ability to reject personalization in the case of gatekeeper platforms, this may mean they have to delete their social media account or use a less accurate map service.[374] Nevertheless, it is still uncertain what effect DMA provisions will have on consumers.

Thirdly, the transparency paradigm would include communicating the costs of using the publisher's digital services and content. Upon entry into force of the DSA and DMA, the consumer protection framework of the EU would apply to the contracts for digital services and content that are monetized via personal data via targeted advertising, as discussed in Part III.B.[375] Nevertheless, personal data itself must not be considered a commodity for which consumers can pay.[376] However, central to consumer protection is that the consumers understand the "price" they pay for services and products.[377] It seems that in the case of targeted advertising, this requirement is equated with the requirement that the nature of monetization is explained in terms and conditions.[378] However, this obviously does not grant the same level of protection to such contracts. For example, Apple's App Store has a listing of apps that are priced, and a listing of "Free Apps" that consumers can download by pressing the "GET" button.[379] Indeed, the description of these free apps contains a disclosure that they are monetized by advertising, but the information on such costs is nothing

371. *See* Lemley, *supra* note 224, at 1268–69.

372. This can easily be confused with the consent for the processing of personal data under the GDPR and ePrivacy Directive. However, consent in the context of personal data and privacy protection is only one of several legal grounds for processing. Opt-in discussed in this paragraph refers to the consumer's choice to receive digital services and content personalized or non-personalized regardless of what data is being processed for personalization, and on what grounds under the GDPR, (i.e. legitimate interest, consent, contractual necessity).

373. *See* Digital Markets Act, *supra* note 28, ¶ 36.

374. *See* TRZASKOWSKI, *supra* note 35, at 185.

375. *See* Digital Content Directive, *supra* note 40, ¶ 73.

376. This also seems to be the case, as interpreted in the recitals of DCD. *See* Digital Content Directive, *supra* note 40, ¶ 24.

377. *See* Guidance on Consumer Rights Directive *supra* note 207, at 35.

378. *See* Digital Content Directive, *supra* note 40, art. 2, ¶ 7.

379. *See App Store*, APPLE, https://www.apple.com/app-store/ (last visited Feb. 12, 2023) [https://perma.cc/JH5D-XTPT] (archived Feb. 12, 2023).

like the obvious reference to the monetary price in the download button for paid apps. For such cases, the Commission can consider constructing a requirement that would be similar to price disclosure. Potentially, this would include the monetary value the publisher earns from processing the personal data of a consumer on average.[380] This could also take the form of a disclosure message that it "monetizes personal data," similar to that for "in-app purchases."

Fourthly, the transparency paradigm itself has limitations, and communicating to consumers about the stakes of giving away their data, and about their rights, is not enough to guarantee fairness in the digital environments. There has been a proliferation of scientific articles and studies that demonstrate that online interfaces can be designed to manipulate, coerce, and even trigger addiction.[381] Such dark patterns have also been applied to trick consumers into sharing data (when entering websites and apps of publishers that are monetized via targeted advertising), burying key terms in dense terms and conditions, and disguising ads via, for example, native ads (advertisements that look like editorial content).[382] The European Data Protection Board provides guidelines for avoiding dark patterns in the context of social network platforms.[383] Moreover, while the DSA dark pattern prohibition excludes situations discussed in this Article, it can clarify what can be considered a dark pattern when consumers make a choice to give consent for data processing.[384] However, further elaboration is likely needed to provide all publishers with the defining design guidance about constructing, for example, cookie consent banners.[385] These guidelines should be explicit, for example, suggesting that "accept all" and "reject optional cookies" must be presented in an equal manner, in the same color, size, and shape. It may be best to provide a user-friendly tool enabling consumers to report websites that may not comply with dark pattern rules.[386]

---

380. *See*, *e.g.*, Malgieri & Custers, *supra* note 250, at 290.

381. *See generally*, *e.g.*, Leiser, *supra* note 262; *see also* EC STUDY ON DARK PATTERNS AND MANIPULATIVE PERSONALISATION, *supra* note 33; Michael Toth, Nataliia Bielova & Vincent Roca, *On Dark Patterns and Manipulation of Website Publishers by CMPs*, 3 PROC. ON PRIV. ENHANCING TECH. 478 (2022); FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT (2022).

382. *See FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers*, FED. TRADE COMM'N (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers [https://perma.cc/TD86-59ZT] (archived Feb. 12, 2023).

383. EUR. DATA PROTECTION BD., GUIDELINES 3/2022 ON DARK PATTERNS IN SOCIAL MEDIA PLATFORMS INTERFACES: HOW TO RECOGNIZE AND AVOID THEM (2022).

384. *See* Digital Services Act, *supra* note 41, ¶ 67.

385. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47, at 26.

386. *See id.* In the United States, users are enabled to report websites containing dark patterns to their respective Attorney General. *See Report A Dark Pattern*, DARK PATTERNS TIP LINE, https://darkpatternstipline.org/report/ (last visited Sept. 15, 2022) [https://perma.cc/FN3V-MQJJ] (archived Feb. 12, 2023).

Fifth, the Commission can consider updating Annex I of the UCPD, or the list of prohibited practices, to reflect the rules of the DSA, DMA, and PAIA. CJEU's pending preliminary ruling about the TCF[387] may result in de facto outlawing the real-time bidding format in the open display market of targeted advertising.[388] The DSA's prohibition of targeted advertising based on special categories of data,[389] coupled with the CJEU's C-184/20 judgment about sensitive inferences,[390] may create a de facto ban on behavioral advertising in its entirety. In any case, UCDP's Annex I is the place to list prohibited practices. In this case, the Commission may use this opportunity to clarify the exact limits of targeted advertising in the EU.

Sixth, evaluating practices in the digital environment to be "misleading" or "aggressive" requires updating the consumer image that is used as a benchmark. As described in Parts III.A and III.C, the UCPD contains the benchmarks of the "average targeted consumer" and the "average vulnerable consumer," revealing a regulatory decision not to regard all behavioral exploitation as a failure of the market that needs correction (e.g., puffery).[391] The Article joins the calls of other scholars arguing for a shift in the enforcement of the UCPD to take into account the universal vulnerability of the digital consumer.[392] While the UCPD is sufficiently flexible, and such interpretations can be left to the national authorities and the CJEU, proactive clarifications by the European legislator can guide further technological developments to a high level of protection for European consumers in digital environments. This is particularly important with the advent of immersive technologies that will have significant effects on consumers' experiences, including the extent to which they can be influenced. This Article further recognizes the need for developing a taxonomy of vulnerabilities that includes different degrees of consumer vulnerability.

---

387. *See IAB Europe Case: The Market Court refers preliminary questions to the Court of Justice of the EU*, *supra* note 142.

388. *See* Veale & Borgesius, *supra* note 18, at 226–27.

389. *See* Digital Services Act, *supra* note 41, ¶ 69.

390. *See* Case C-184/20, *supra* note 304, ¶ 123.

391. *See* Unfair Commercial Practices Directive, *supra* note 37, art. 5(2)(b)–(3). The "average targeted consumer" is generally accepted shorthand for "the average member of that group," "where a commercial practice is directed to a particular group of consumers." OFF. OF FAIR TRADING, DEP'T FOR BUS., ENTER. & REGULATORY REFORM, CONSUMER PROTECTION FROM UNFAIR TRADING: GUIDANCE ON THE UK REGULATIONS 69 (2008), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file /284442/oft1008.pdf [https://perma.cc/YQF7-3WLN] (archived Feb. 12, 2023). The "average vulnerable consumer" is a member of a "clearly identifiable group of consumers is particularly vulnerable to the practice or to the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee." *Id.* at 70.

392. *See* Helberger, Borgesius & Reyna, *supra* note 35; *see also* Laux, Wachter & Mittelstadt, *supra* note 319; GALLI, *supra* note 35, at 188–92; TRZASKOWSKI, *supra* note 35.

Lastly, this Article is focused on providing an overview of the substantive rules of consumer protection that limit targeted advertising in the EU. However, available and unavailable remedies, as well as enforcement challenges of the consumer protection rules, are also important areas for the fitness check of the consumer protection framework. For example, while DCD has introduced the right to repair and refund for consumers of publishers that monetize their services and content via targeted advertising, what exactly such remedies entail is quite unclear.[393] In general, applying consumer protection may mean double liability for the publishers.[394] For example, suppose a search engine is in breach of adequate consent requirements under the GDPR. In that case, it could also be seen as a breach of contract under the CRD, entitling the application of national contract law remedies such as contract termination and damages.[395] Moreover, such a breach may also constitute an unfair commercial practice under the UCPD, leading to fines.[396] The existing consumer protection framework that is applicable to targeted advertising (in particular the UCPD, CRD, and UCTD) primarily relies on the member states to ensure the enforcement of substantial provisions.[397] However, the Commission recognizes the risks affecting the collective interests of consumers in the EU due to globalization and digitalization, but also misleading advertisements and unfair contractual terms, introducing Directive (EU) 2020/1828 on Representative Actions.[398] Moreover, Regulation (EU) 2017/2394 on Consumer Protection Cooperation provides a tool for cooperation when publishers and consumers are not established in the same country.[399] The DSA introduces other enforcement mechanisms, consisting of national and EU-level cooperation, where each member state will need to appoint a digital services coordinator, an independent authority that will be responsible for supervising the intermediary services established in their country.[400] The Commission will have direct oversight and enforcement authority over very large online platforms and can, in the most serious situations, impose fines of up to 6 percent of their global

393. *See* Digital Content Directive, *supra* note 40, ¶ 73.

394. *See* Leiser, *supra* note 262.

395. *See* Regulation 2017/2394, of the European Parliament and of the Council of 12 December 2017 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws and Repealing Council Regulation 2006/2004, 2017 O.J. (L 345) ¶ 17 [hereinafter Consumer Protection Cooperation Regulation].

396. *See Guidance on the Unfair Commercial Practices Directive*, *supra* note 257, at 99–101.

397. *See* EU Report Targeted Advertising & Informed Consent, *supra* note 47.

398. Directive 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, 2020 O.J. (L 409) 1.

399. *See generally* Consumer Protection Cooperation Regulation, *supra* note 395.

400. *See* Digital Services Act, *supra* note 41, ¶ 109.

revenue.[401] However, the enforcement framework may not be able to remove all obstacles to cross-border collective action, leaving cross-border enforcement as one of the central challenges of the consumer protection law framework in the EU.

IV. CONCLUSIONS

Consumer protection legislation is a central framework for regulating targeted advertising, particularly in regard to consumer manipulation. It limits targeted advertising in both stages: when consumers access digital content and/or services monetized by targeted advertising and when consumers are presented with personalized advertising. At both stages, consumer protection rules prescribe provisions not only for transparency so as to empower the consumer that may be the weaker party in commercial dealing, but also for protecting them beyond transparency by assessing the fairness of commercial practices. The EU has increased the normative position of consumers by introducing further rules in the DSA, DMA, and PAIA that affect targeted advertising. In particular, the DSA prohibits dark patterns as well as targeted advertising based on special categories of data (e.g., health or political affiliation), as well as targeted advertising directed towards minors. Additionally, the DSA includes transparency requirements for online platforms to disclose targeting criteria and further requires very large online platforms to keep a repository of advertisements. This will enable regulators and other interested observers to scrutinize targeted advertising practices ex post. The UCPD is particularly important in providing such ex post analysis in its three-layered test of unfairness for commercial practices.

Overall, when complemented with personal data protection, privacy, non-discrimination, and competition rules, the consumer protection framework in the EU provides a valuable tool to address harms stemming from targeted advertising. Nevertheless, there are some legislative gaps that the Commission must fill in order to enforce consumer protection rules more effectively. This Article provides an overview of the consumer protection framework in the EU and how it regulates targeted advertising. Moreover, it sheds some light on the gaps in the framework and provides recommendations for the Commission to fill them.

401. *See id.* art. 52.