



Towards a more transparent, balanced and sustainable digital advertising ecosystem:

Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers

Final Report

Written by Catherine Armitage, Nick Botton,
Louis Dejeu-Castang, Laureline Lemoine (AWO Belgium)

A W O

Internal identification

Contract number: LC-01712891

VIGIE number: VIGIE 2020-0663

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

Directorate H — Digital Society, Trust and Cybersecurity

Unit H.2 — Cybersecurity and Digital Privacy Policy

Contact: CNECT-H2@ec.europa.eu

European Commission

B-1049 Brussels

Towards a more transparent, balanced and sustainable digital advertising ecosystem:

Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers

***EUROPE DIRECT is a service to help you find answers
to your questions about the European Union***

Freephone number (*):
00 800 6 7 8 9 10 11

(* The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. The Commission does not guarantee the accuracy of the data included in this study. More information on the European Union is available on the Internet (<http://www.europa.eu>).

PDF

ISBN: 978-92-76-61811-9

doi: 10.2759/294673

Catalogue number: KK-04-23-015-EN-N

Manuscript completed in October 2022

First edition

Luxembourg: Publications Office of the European Union, 2023

© European Union, 2023



The European Commission is not liable for any consequence stemming from the reuse of this publication.

The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

Table of contents

PART A

1	How has digital advertising evolved over the past 10-15 years?	14
1.1	Description of digital advertising and how it has evolved over the past 10-15 years	14
1.2	Overview of the competitive landscape	21
1.3	Overview of the role and value of data in digital advertising, how this is evolving in light of recent developments and how this is communicated to users	37
1.4	Conclusion	65
2	How has this evolution impacted the privacy of EU citizens, democracy and society in the EU and the environment?	66
2.1	Has the evolution of digital advertising led to a high level of privacy and data protection for EU citizens?	66
2.2	What impact has the evolution of digital advertising had on democracy and society in the EU?	78
2.3	What is the environmental impact of the way that digital advertising has evolved?	89
2.4	How do the efficacy and efficiency benefits of the evolution of digital advertising compare to the societal and environmental impact?	96
2.5	Conclusion	103

PART B

3	Evolution and distribution of advertising spend across the digital advertising ecosystem	104
3.1	Digital vs. traditional advertising	104
3.2	Bulgaria	105
3.3	Czechia	106
3.4	Germany	107
3.5	Greece	108
3.6	Spain	108
3.7	France	109
3.8	The Netherlands	109
3.9	Poland	110
3.10	Slovenia	111

3.11 Finland	111
3.12 Conclusion	112
4 Advertisers' and publishers' experiences	113
4.1 Benefits of digital advertising for advertisers and publishers	114
4.2 The relationship between publishers and advertisers, major platforms and intermediaries	120
4.3 Other key issues identified by advertisers	125
4.4 Other key issues identified by publishers	130
4.5 Conclusion	136
4.6 Interview methodology	136
PART C	
5 Alternative digital advertising models	138
5.1 Contextual advertising	141
5.2 Local profiling models	157
5.3 Other emerging digital advertising proposals	177
5.4 Subscriptions	183
5.5 Key findings	190
6 Ways for individuals to indicate their preferences for data collection and targeting	194
6.1 Introduction	194
6.2 The GDPR and the proposed ePrivacy Regulation	197
6.3 Industry tools	199
6.4 Google Ad Settings	204
6.5 Facebook Ad Preferences	211
6.6 The European Interactive Digital Advertising Alliance's Your Online Choices tool	219
6.7 Apple's App Tracking Transparency Framework	225
6.8 Key findings	227
7 How does the existing regulatory framework address the issues raised in this study?	229
7.1 The General Data Protection Regulation	229
7.2 ePrivacy	232
7.3 EU competition law	233
7.4 Environmental initiatives	235
7.5 Digital Markets Act	236
7.6 Digital Services Act	238
7.7 EU consumer protection law	243

8	Areas for further analysis	245
8.1	Transparency: summary of the issues	245
8.2	Allowing advertisers and publishers to know their audience	257
8.3	Allowing consumers to choose whether and how to be targeted with ads	260
9	Conclusion	263
ANNEX		
	Annex 1: Glossary	265
	Annex 2: Additional research areas	271

Abstract

This study has collated evidence which on balance indicates a strong case to reform digital advertising. It indicates that the status quo is unsustainable for individuals, publishers and advertisers. Digital advertising that relies on the collection of personal data, tracking and massive-scale profiling can have unintended consequences on data protection rights, security, democracy and the environment. But there is little independent evidence to support claims that the use of extensive tracking and profiling yields a significant advantage compared to digital advertising models which don't do this. This strengthens the position of players who have the most control over and insight into people's behaviour online and weakens the ability of others, especially advertisers and publishers, to communicate directly to their customers. It has also created an accountability crisis, where individuals are expected to navigate a complex web of companies in order to control the types of ads they see online. This study points to gaps in the regulatory framework which could enable many of the issues highlighted to persist. There is a need to improve transparency and accountability, increase individuals' control over how their personal data is used for digital advertising and address a number of obstacles that make it harder for advertisers and publishers to "know their audience".

Executive Summary

Since the first online banner ad was placed in 1994, the digital advertising ecosystem has been significantly transformed as the size of the global industry has grown. Digital is the largest advertising channel in the European Economic Area (EEA), generating more revenue than all other advertising channels combined. Digital advertising is often seen as an important, if not essential, way of funding online content without requiring payment from individuals. In principle, advertising has always been 'targeted' to some extent, in the sense that marketers make rational decisions on segmenting and targeting before purchasing ad space. However, only recently has targeted advertising become associated with pervasive digital tracking and with 'creepy' or persistent ads over which individuals feel they have no control.

Over the past 10-15 years, search advertising and social media advertising channels, where large platforms play key roles, have grown at an extremely rapid rate compared to the channel which directs the most advertising revenue towards publishers ("other" display). Some large platforms can generate advertising revenue both as a publisher (by selling ad inventory on the platforms and services they own) and as an intermediary (by providing advertising technology services to advertisers and other publishers). The combined revenue of the largest European publishers has stagnated over the past ten years, while Alphabet (Google) and Meta's revenues increased by more than 500% during the same period. The evidence in this study indicates that this is due to lack of transparency and large and growing imbalances in bargaining power, not due to existing or proposed rules on privacy and data protection.

The way that digital advertising is bought and sold can be extremely complex. Advertisers and publishers, especially large ones, often work with a range of intermediaries – sometimes referred to as "ad tech" companies - to buy and sell advertising through different channels. This complexity has given rise to concerns about transparency, cost, security, privacy, data protection and competition.

The most widely used products in digital advertising rely on large amounts of personal data and profiling of individuals. Personal data is used for targeting and measuring advertising campaigns, often tied to common identifiers that enable companies to build up a picture of an individual's behaviour across sites, apps, platforms and devices.

The large amount of data processing required to support the most widely used digital advertising methods leads to high energy consumption and emissions. A significant amount of this data processing is likely to be linked to fraudulent activity and waste that does not generate any value for advertisers.

Individuals do not have adequate control over how their personal data is collected and used for digital advertising. Our assessment suggests that several industry tools which offer people control over their personal data are not user-friendly. This is compounded by the fact that individuals are required to indicate their preferences across all of these tools separately in order to influence the way that ads are targeted to them across the different devices, apps and sites they use: this is confusing and difficult to understand.

There is limited evidence to suggest that the efficiency and efficacy gains of advertising products that rely on personal data and profiling outweigh the interference with individuals' fundamental rights and consumer rights in addition to the reported negative societal impacts. A large amount of academic research has focused on demonstrating that the way that digital advertising works today has significant impacts on privacy, data protection, democracy, society and the environment. However, there is a lack of independent analysis to assess the costs and benefits of using personal data and profiling in advertising.

European publishers struggle to compete for digital advertising revenue because large platforms have more access to data than they do. Over the past ten years, European publisher revenues have stagnated or declined while large platform revenues have increased. A significant amount of digital advertising revenue flows towards large platforms which compete with publishers to sell ad space next to the content they host, as well as providing intermediary services for publishers and advertisers to buy and sell ads. This dual role creates a "frenemy" dynamic, with some publishers saying that they would lose advertising revenue if they did not work with these large platforms.

This has created an unsustainable situation for advertisers and publishers. Advertisers and publishers often describe the relationship with large platforms in negative terms and describe a sense of "dependency". Some advertisers and publishers are concerned that moves by large platforms to limit access by other companies to data generated through the use of their platforms and operating systems on what they claim to be privacy and data protection grounds will result in less transparency and less competition in digital advertising in the future.

Lack of transparency in digital advertising limits evidence-based decision-making because advertisers lack independent data to assess the

performance of digital advertising. This strengthens the position of players with strong market power and deters advertisers from switching to emerging alternatives that are less intrusive, even though there is evidence that some advertisers would prefer to rely on models that minimise the processing of unnecessary personal data. More independent data about the performance of alternative models compared to the status quo is needed to encourage widespread adoption among advertisers and publishers.

The European Union's (EU) current regulatory framework, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive, addresses some of these issues to a limited extent, **but specific features of the digital advertising ecosystem – in particular the rapidly changing and complex nature of personal data processing in this context – can present barriers to effective enforcement.** Proposed instruments such as the Digital Services Act (DSA) and the Digital Markets Act (DMA) include provisions related to some issues, such as transparency (both B2B and consumer), but it is unclear to what extent these will have a concrete impact on the digital advertising ecosystem and the issues highlighted in this study in practice.

Overall, there is a need to **improve transparency and accountability** in the digital advertising ecosystem in three particular areas: ad spend and other B2B issues; the collection, use and dissemination of personal data; and environmental impacts. There is a need to **increase individuals' control over how their personal data is used for digital advertising**, including how they avoid unwanted targeting. There are also a number of **obstacles that make it harder for advertisers and publishers to "know their audience"** and communicate with them directly through advertising. This study recommends that these areas be the focus of future reflection and analysis, whether in the form of further research or options for future policy interventions, in order to address the various and considerable issues which have been identified.

Study objectives

The purpose of this study is to assemble evidence on the digital advertising industry that could inform future policy options for safeguarding individual privacy and supporting the evolution of a more balanced digital advertising ecosystem.

The study has three specific objectives. The first objective is to describe how digital advertising has evolved over the past 10-15 years and how this has impacted European publishers and advertisers (large and small). This includes assessing, based on independent and objective evidence, the efficacy and efficiency of digital advertising with respect to its societal and environmental impact.

The second objective is to assess the extent to which there is an imbalance in the relationship between publishers and advertisers, on the one hand, and the major platforms and digital advertising intermediaries on the other.

The third objective is to inform the development of options for promoting and supporting a more transparent and balanced digital advertising ecosystem that (a) is more respectful of the Charter of Fundamental Rights, in particular the right to privacy (b) pays particular attention to the vulnerability of children and young people (c) supports a free and good quality press and independent media (d) minimises waste and environmental impact (e) complements related parts of the regulatory framework, including the proposed Digital Services Act package.

Tasks and methodology

To address the three objectives outlined above, several tasks were carried out based on a series of research questions:

- 1) How has digital advertising evolved over the past 10-15 years?
- 2) How has this evolution impacted (a) the revenues of different players in the digital advertising ecosystem (b) competition in European digital advertising markets (c) the privacy of EU citizens (d) democracy and society in the EU (e) the environment?
- 3) How has the distribution of advertising spend evolved across the digital advertising ecosystem over the past 10 years?
- 4) How do advertisers and publishers describe their relationships with large platforms and digital advertising intermediaries? What positive and negative aspects do they identify in relation to the way the current digital advertising ecosystem functions?
- 5) What would a more transparent and balanced digital advertising ecosystem look like? What alternative models exist, how viable are they and how could use of these models be incentivised (including through regulatory and economic interventions)?

To address question 1, we carried out quantitative analysis of advertising spend data at global and EEA level based on estimates developed by four major global advertising agency networks. We also analysed public filings, annual reports and other publicly available documents published by European publishers and large platforms. To develop an overview of the role and value of data in digital advertising, including how this is evolving in light of recent developments and how this is communicated to users, we carried out desk research and consulted experts. We also reviewed how data collection methods for advertising purposes are covered by companies' terms of service and privacy policies.

To address question 2, we carried out a literature review of relevant studies and papers related to digital advertising and its impact on the areas outlined in the research question. We also consulted experts including advertisers, publishers, civil society organisations, regulatory authorities (including competition and data protection authorities), trade associations and relevant industry experts.

To address question 3, we carried out quantitative analysis of advertising spend data in ten Member States. We also carried out desk research to find additional information published by industry bodies, trade associations and other local sources.

To address question 4, we carried out interviews with small and large advertisers and publishers, as well as several relevant trade associations.

To address question 5, we carried out a review of different digital advertising models according to specific criteria related to the use of monitoring and profiling, sensitive data and third-party data sharing. This involved desk research and interviews with experts, including advertisers, publishers, relevant trade associations and providers and developed of alternative digital advertising models. We also reviewed a number of different tools that offer individuals ways to see and control how their personal data is used for digital advertising purposes. We also carried out an assessment of how the existing regulatory framework addresses some of the issues raised in the study and outlined a number of areas of focus for future reflection and analysis, based on desk research and consultation with a wide range of stakeholders including advertisers, publishers, relevant trade associations, large platforms, industry experts, regulatory authorities (including data protection and competition authorities) and relevant civil society organisations.

In September 2022, a workshop was held to inform relevant stakeholders and experts about the progress of the draft study and get feedback. 41 participants attended the workshop, which focused on four areas: (1) transparency and efficiency in digital advertising (2) privacy and data rights (3) reducing waste in the digital advertising market (4) creating a more balanced advertising ecosystem.

An advisory board was set up following a list of experts identified at the proposal stage of the study. The experts that we included in the list covered a variety of different expertise and backgrounds (academia, industry, civil society). The selection of the experts was agreed with the European Commission, and it included the following people: Wayne Blodwell, Bob Hoffman, Mikko Kotila, Michael Veale and Clare Melford. They were asked to review and provide feedback on drafts of the study at various stages throughout the drafting process. Members of the advisory board were also invited to participate in the study workshop that took place in September 2022.

Part A

How has the evolution of digital advertising over the past 10-15 years impacted (a) the revenues of different players in the digital advertising ecosystem (b) competition in European digital advertising markets (c) the privacy of EU citizens (d) democracy and society in the EU (e) the environment?

1 How has digital advertising evolved over the past 10-15 years?

This section looks at how digital advertising has evolved over the past 10-15 years, and how this evolution has impacted the revenues of different players and competition in the European Union (EU).

1.1 Description of digital advertising and how it has evolved over the past 10-15 years¹

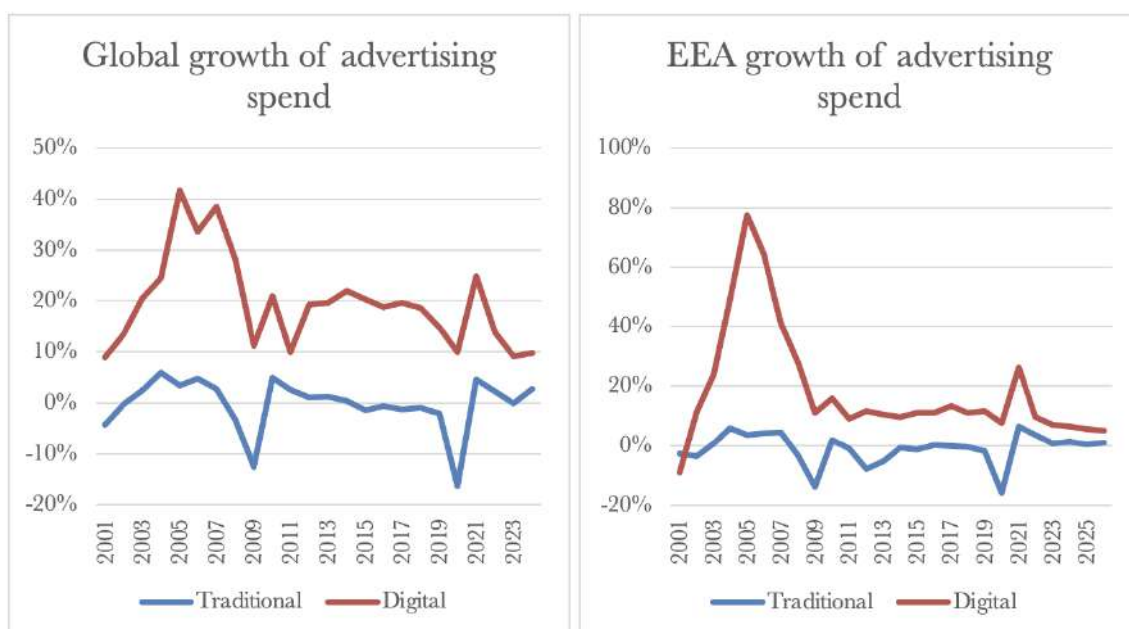
Over the past 10-15 years, digital has evolved to become the biggest advertising channel in the European Economic Area (EEA), generating more advertising revenue than all other channels combined. Search advertising and social media advertising channels, where large platforms play key roles, have grown at an extremely rapid rate compared to the channel which directs the most advertising revenue towards publisher sites ("other" display).

¹ Advertising spend data in section 1 is based on the latest figures available when the analysis was carried out in Q1 2022. This data and other contributions to this section were collated by Dietmar Kruse.

1.1.1 Ad spend: digital vs traditional

Since the first online banner ad was placed in 1994², the digital advertising ecosystem has been significantly transformed as the size of the global industry has grown (from about €99 million in 1995³ to €357 billion in 2021)⁴. Digital became the largest advertising channel globally in 2016, overtaking television. In the European Economic Area (EEA), €46 billion was spent on digital advertising in 2021, more than on all other advertising channels combined⁵.

Globally and in the EEA, digital advertising spend has seen double-digit growth almost every year since 2002 (figure 1). By contrast, spend on traditional advertising channels such as TV, magazines, radio, cinema and outdoor⁶ has been in relative decline since 2001, showing much lower growth rates⁷.



² Wasserman T, 'This is the World's First Banner Ad' (2013) <<https://mashable.com/archive/first-banner-ad>>.

³ Calculated based on the 1999 end-of-year exchange rate (€1=\$0.99), the year the Euro was introduced. All subsequent exchange rate calculations are based on the end-of-year exchange rate from the year the data in question was sourced from. All exchange rate data was sourced from Google Finance. Zenith Advertising Expenditure Forecasts, December 2021.

⁴ Zenith Advertising Expenditure Forecasts, December 2021.

⁵ Data excludes Cyprus, Iceland, Lichtenstein, Luxembourg and Malta. WPP (December 2021).

⁶ Advertising on television and radio covers advertising as part of scheduled broadcasts, as opposed to advertising on connected TV (which counts as digital). Only advertising on printed editions is taken into account for newspaper and magazine advertising. Out-of-home covers billboards, posters and other place-based advertising.

⁷ Zenith Advertising Expenditure Forecasts December 2021.

Figure 1: Annual growth of advertising spend globally and in the EEA (excluding Cyprus, Iceland, Lichtenstein, Luxembourg and Malta). Source: Zenith Advertising Expenditure Forecasts December 2021 (Global data) and WPP (December 2021) (EEA data).

1.1.2 Structure of the digital advertising ecosystem

Digital advertising is usually categorised by industry analysts into four types, often referred to as “channels”: search, social media, “other” display, and classified⁸.

1.1.2.1 Search advertising

Search advertising is the biggest digital advertising channel in the EEA (39% of digital advertising spend – €17 billion)⁹ though it is only the second largest channel globally.

Search advertising usually takes the form of sponsored entries which appear within a list of search results on a search engine website and are typically labelled as ads or sponsored content. Search ads are typically delivered to users based on keywords associated with their individual searches, although other types of data can be used to supplement the targeting of search ads.

In its study on the digital advertising sector in Spain, the Spanish competition authority, Comisión Nacional de los Mercados y la Competencia (CNMC), estimated that Google’s share of the search advertising market in Spain was over 90% in 2019, with the next largest competitor, Microsoft’s Bing, representing less than 10% and all other competitors put together representing less than 5% of the market¹⁰. The French competition authority, Autorité de la Concurrence (ADLC), similarly estimated that Google’s share in the search advertising market was at least 70% in France in 2018¹¹.

Search advertising is usually bought directly from the search engine provider or via a media agency, with larger advertisers being more likely to buy through an agency.

⁸ Omnicom, MagnaGlobal and Zenith use these categories in their industry analysis reports.

⁹ Calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal. The data provided by GroupM, Omnicom and MagnaGlobal is sourced from internal databases that are only available to their clients. They have agreed to allow the data to be used as part of this study, on the condition that the datasets underlying the aggregated and averaged data displayed in this study are not publicly shared. This applies to all data sourced from GroupM, Omnicom and MagnaGlobal displayed in this study.

¹⁰ ‘E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain’ (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

¹¹ ‘Avis N° 18-A-03 Du 6 Mars 2018 Portant Sur l’exploitation Des Données Dans Le Secteur de La Publicité Sur Internet’ (Autorité de la concurrence, 6 May 2018) <<https://www.autoritedelaconcurrence.fr/sites/default/files/2019-05/18a03.pdf>>.

1.1.2.2 Social media advertising

Social media advertising is one of the fastest growing digital advertising channels. It typically either takes the form of in-feed ads (which blend in with content on the platform), display banner ads or video ads (e.g. before a video begins) placed on social media websites or apps. These ads are typically targeted based on users' personal data, such as information about their interests (see section 1.3.2 for more detail).

Social media advertising is often bought directly from the social media provider. Meta has a proprietary "Ads Manager" tool that enables advertisers and their agencies to create ads, manage when and where they are placed and track performance¹² across different Meta platforms including Facebook, Instagram and Messenger. Other social media providers enable advertisers to buy ads in a number of different ways. TikTok has an "Ads Manager" tool which enables advertisers and their agencies to create ad campaigns and track engagement such as clicks and conversions. YouTube ads can be bought directly using Google's proprietary tool ("Google Ads") or through more complex auction-based systems known as "programmatic buying" (see section 1.1.2.4).

1.1.2.3 Classified advertising

Classified advertising represents a very small part of global and EEA digital advertising spend (6-7%)¹³. It refers to advertising by individuals and companies listed on a regional or local level, primarily on a customer-to-customer basis.

1.1.2.4 "Other" display advertising

"Other" display advertising refers to display advertising on all websites and apps other than social media and search engines. It typically takes the form of display banner ads or video ads. The largest providers are publishers¹⁴ such as broadcasters and online newspapers, along with large platforms that are not social media or search engine providers (for example, Amazon). Some stakeholders, including some competition authorities, refer to a part of the "other" display

¹² 'Facebook Ads Manager: Ads Management for Facebook, Instagram' (*Meta for Business*) <<https://www.facebook.com/business/tools/ads-manager>> accessed 5 June 2022.

¹³ Calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal. See footnote 9.

¹⁴ The term "publisher" is often used in a digital advertising industry context to mean an entity that receives revenue from making advertising space available on websites, apps and other platforms that they own. This can include broadcasters, radio stations, newspapers, magazines, gaming and streaming platforms (e.g. Twitch), e-commerce sites (e.g. Amazon) and also large platforms such as Google and Meta. Google and Meta earn advertising revenue both as publishers and providers of advertising technology services (intermediaries) in the programmatic supply chain. However, neither company publishes data about how much advertising revenue they earn as publishers compared to as intermediaries. This is why this study will refer to Google and Meta separately as "large platforms". See section 1.2.2.1 for a more detailed discussion on this.

advertising market as the “open display market”, defined as a market in which “a wide range of publishers sell advertising space to advertisers through a complex chain of third-party intermediaries that run auctions on behalf of the publishers and advertisers”¹⁵. “Open display” represented 41-42% of the “total display” market¹⁶ in Spain¹⁷ in 2019. In the UK, “open display” represented 30-35% of the “display advertising” market in 2020¹⁸.

In the early days of digital advertising, display advertising was bought directly from publishers. Deals were arranged directly and advertisers (sometimes via agencies) would buy a fixed amount of impressions at a fixed price (known commonly as cost-per-mille (CPM), a term used to denote the cost per thousand impressions). Subsequently, advertising networks emerged as a way for advertisers to buy advertising from a group of publishers, rather than having to do deals with each one individually. Advertising networks served as brokers, enabling advertisers to buy a specific amount of impressions for a fixed price and have them delivered across multiple publishers.

As the number of publishers selling advertising online increased, programmatic advertising eventually began to replace ad networks as an automated way of buying and selling digital ad space across multiple websites and publishers in real time. Programmatic advertising promised to reduce the costs, inefficiencies and limitations of traditional systems that relied on human ad buyers and salespeople¹⁹.

¹⁵ ‘Online Platforms and Digital Advertising Market Study - Glossary’ (Competition & Markets Authority, 2020) <https://assets.publishing.service.gov.uk/media/5efc5cad3a6f4023d3b7a866/Final_Report_Glossary.pdf>.

¹⁶ The “total display market” should be understood as a combination of the “other” display market and the social media advertising market.

¹⁷ ‘E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain’ (*Comisión Nacional de los Mercados y la Competencia*, 7 July 2021), p. 82 <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

¹⁸ ‘Online Platforms and Digital Advertising - Market Study Final Report’ (*Competition and Markets Authority*, 2020), p. 246 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

¹⁹ Marshall J, ‘WTF Is Programmatic Advertising?’ (*Digiday*, 20 February 2014) <<https://digiday.com/media/what-is-programmatic-advertising/>> accessed 5 June 2022.

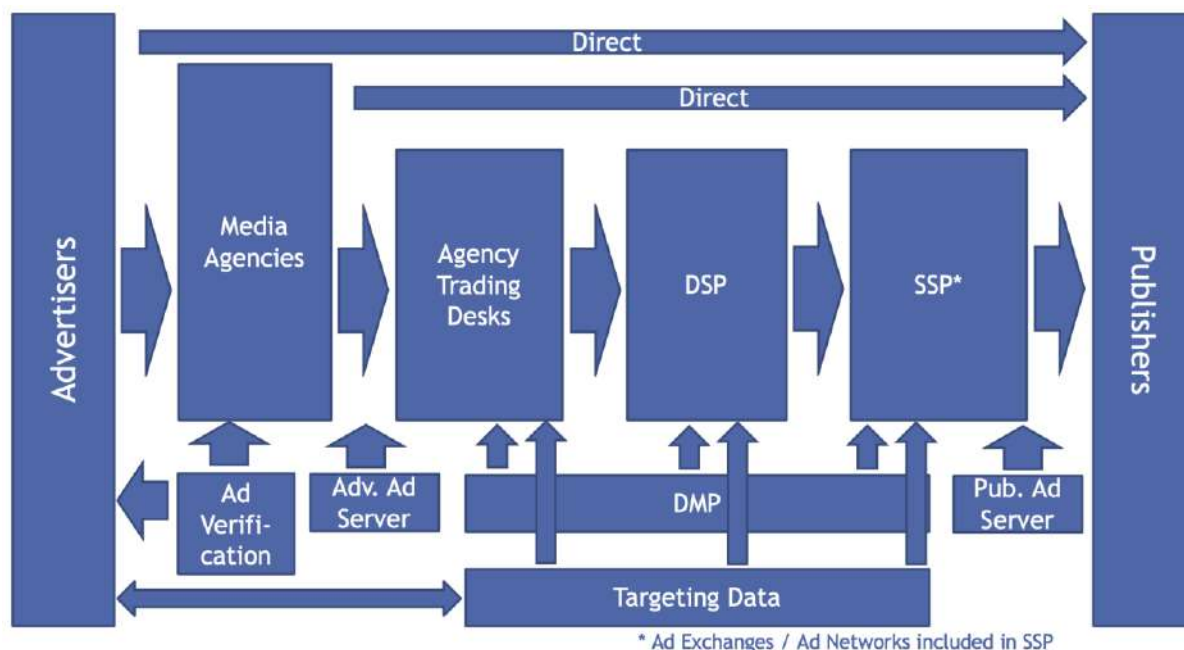


Figure 2: Simplified scheme of the programmatic advertising value chain. Source: Dietmar Kruse.

Hailed as “the future of marketing”²⁰ when it was first developed, programmatic advertising uses technology to “automate and optimise, in real time, the ad buying process”²¹. This automation is made possible by two key additional layers in the system:

- 1) Demand-side platforms (DSPs) which enable advertisers and agencies to automate the buying of digital advertising.
- 2) Supply-side platforms (SSPs) used by publishers to manage, sell and optimise advertising space (also known as inventory) on their websites, mobile apps and other digital properties in an automated way. Competition authorities in the UK (the Competition and Markets Authority, or CMA)²² and Australia (the Australian Competition and Consumer Authority, or ACCC)²³ have both noted that SSPs today also perform functions which used to sit separately under “ad exchanges”, namely facilitating the buying and selling

²⁰ Rayport JF, ‘Is Programmatic Advertising the Future of Marketing?’ (*Harvard Business Review*, 2015) <<https://hbr.org/2015/06/is-programmatic-advertising-the-future-of-marketing>> accessed 5 June 2022.

²¹ ‘Glossary of Terminology’ (*IAB*) <<https://www.iab.com/insights/glossary-of-terminology/>> accessed 7 June 2022.

²² Online Platforms and Digital Advertising - Market Study Final Report’ (*Competition and Markets Authority*, 2020), p. 19, 264 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

²³ ‘Digital Advertising Services Inquiry Final Report’ (*Australian Competition and Consumer Authority*, 2021), p. 31 <<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

of advertising inventory using auction-based systems to determine the price of inventory according to parameters set by publishers and advertisers.

Today, “other” display advertising can be bought programmatically or via direct deals with publishers (see figures 2 and 3).

	Mechanism	Market	Buying Model	Inventory Type	Pricing
PROGRAMMATIC	RTB	OPEN	Open Market (RTB)	One to Many (Unreserved)	Dynamic (RTB Auction)
		PMP	Private Marketplace (PMP)	One to Few (Unreserved)	Dynamic (RTB & Price Floor)
	PROGRAMMATIC DIRECT		Preferred Deals	One to One (Unreserved)	Fixed Rate
			Automated Guaranteed	One to One (Reserved)	Fixed Rate
			Programmatic Guaranteed	One to One (Reserved)	Fixed Rate
DIRECT		Insertion Order	One to One (Reserved)	Fixed Rate	

Figure 3: Types of digital advertising and buying models. Source: TPA Academy.

1.1.3 Evolution of different channels

In 2014, the majority of digital advertising spend in the EEA was split between search and “other” display. Spend on social media advertising has increased rapidly since then, growing by 617% between 2014 and 2021 (88% per year on average)²⁴. All channels have shown high growth rates over the past eight years, but “other” display has grown at a slower rate than search and social media advertising²⁵. Industry forecasts indicate that spend on search and social media advertising in the EEA is expected to grow by an annual rate of 8-12% over the next the years, compared to just 4% for “other” display advertising.

At a global level, the growth of social media advertising has been even faster (1,039% between 2014 and 2021, or 148% per year on average) and it is now the biggest advertising channel globally²⁶. Although the global annual growth rates of social media and “other” display advertising have been similar over the past eight years, industry forecasts indicate that spend on “other” display advertising will grow by an annual rate of just 7% over the next three years, compared to 11% for search advertising and 17% for social media advertising.

²⁴ Calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal. See footnote 9.

²⁵ Calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal. See footnote 9.

²⁶ Calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal. See footnote 9.

1.2 Overview of the competitive landscape

Google currently plays a key role in the two biggest digital advertising segments: search and display. Google generates revenues both as a publisher (by selling ad inventory on the platforms and services it owns) and as an intermediary (by providing advertising technology services to advertisers and other publishers)¹. The combined revenue of the largest European publishers has stagnated over the past ten years, while Alphabet and Meta's revenues increased significantly during the same period.

1.2.1 By channel

1.2.1.1 Search advertising

Studies by competition authorities in Spain²⁷, France²⁸ and the UK²⁹ have indicated that in 2019 Google held between 70% (France) and 90% (Spain, UK) of the search advertising market in each country.

1.2.1.2 Display advertising (social media advertising + "other" display)

Although market share data is not available broken down into the sub-categories listed above (social media and "other" display), competition authorities in Spain and the UK have calculated estimates of the overall display market, which combines all sub-categories of display advertising. According to these estimates (see table 1), in 2019, Meta represented over 40% of the "total display" market in Spain, and 35-40% of the "display advertising" market in the UK. "Open display", which is typically defined as the inventory of publishers sold primarily through intermediaries, represented 41-42% of the "total display" advertising market in Spain and 30-35% of the "display advertising" market in the UK. This suggests that in both Spain and UK (the latter being one of the most developed

²⁷ 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (*Comisión Nacional de los Mercados y la Competencia*, 7 July 2021)

<https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

²⁸ 'Avis N° 18-A-03 Du 6 Mars 2018 Portant Sur l'Exploitation Des Données Dans Le Secteur de La Publicité Sur Internet' (*Autorité de la concurrence*, 6 May 2018)

<<https://www.autoritedelaconcurrence.fr/sites/default/files/2019-05/18a03.pdf>>.

²⁹ 'Online Platforms and Digital Advertising - Market Study Final Report' (*Competition and Markets Authority*, 2020)

<https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

advertising markets in Europe), Meta generated more display advertising revenue in 2019 than most other publishers combined.

Meta is currently a key player in display advertising, although new players are emerging. For example, Amazon is a growing player in the display advertising market: media consultancy Ebiqity estimates that its advertising revenue grew by 63% between 2020 and 2021, although this still only represented less than 4% of global digital advertising spend in 2021³⁰. Similarly, TikTok revenues are forecast to increase in 2022 compared to the previous year³¹, nearly all from advertising.

Spain (2019)³²	UK (2019)³³
Open display: 41-42%	Meta: >35-40%
Meta: >40%	Open display: 30-35%
Amazon: <10%	Instagram: 10-15%
YouTube: <10%	YouTube: 5-10%
Twitter: <5%	Other platforms: 5-10%
Spotify: <5%	
LinkedIn: <5%	
Snapchat: <5%	
Pinterest: <5%	
Other: <5%	

Table 1: Overview of market share in the "total display" advertising market in Spain and the "display advertising" market in the UK. Source: Spanish CNMC Study on the 'Competition Conditions in the Online Advertising Sector in Spain' (2021), UK CMA Market Study on 'Online Platforms and Digital Advertising' (2020).

Google plays a role in the display market as a publisher by selling ad inventory on its own properties, such as YouTube, and as an intermediary by providing intermediary services which advertisers can use to place ads on a large number

³⁰ 'Q4 Earnings Are In - The Advertising Revenues of Alphabet, Meta and Amazon in 2021' (Ebiqity plc on LinkedIn) <https://www.linkedin.com/posts/ebiquity-plc_now-that-amazon-has-posted-their-q4-earnings-activity-6895115061984378880-p_sj> accessed 28 June 2022.

³¹ 'The All-Conquering Quaver' (The Economist, 2022) <<https://www.economist.com/interactive/briefing/2022/07/09/the-all-conquering-quaver>> accessed 19 July 2022.

³² 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

³³ 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020) <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

of third-party websites. According to Google, advertisers using its services can place ads on the Google Display Network, “a collection of over two million websites that reach over 90% of internet users across the globe”³⁴. Its annual reports regularly note that ads placed on Google properties have a lower “cost of revenue” than ads placed on the Google Display Network, indicating that Google may have a financial incentive to direct more ad spend towards its own properties than elsewhere³⁵. Between 2018-2021, Alphabet’s advertising revenue generated on Google properties (excluding YouTube) increased by 75% while Google’s display network revenue only increased by 37%³⁶.

1.2.2 By group

This section looks at the dynamics of the relationships in the digital advertising ecosystem between four key groups: publishers, advertisers, media agencies and intermediaries. There is a particular focus on publishers. Section 1.2.2.1 will assess the revenues of publishers compared to large platforms and examine possible explanations for revenue patterns over the past decade.

1.2.2.1 Publishers

The term “publisher” is often used in a digital advertising industry context to mean an entity that receives revenue from making advertising space available on websites, apps and other platforms that they own. This can include broadcasters, radio stations, newspapers, magazines, gaming platforms (e.g. Twitch), e-commerce sites (e.g. Amazon) and also large platforms such as Google and Meta.

³⁴ ‘Reach a larger or new audience with Google Display Network targeting’ (Google) <https://ads.google.com/intl/en_id/home/resources/reach-larger-new-audiences/> accessed 2 June 2022.

³⁵ See ‘Alphabet Annual Report 2021’ (Alphabet, 2021), p. 65 <https://abc.xyz/investor/static/pdf/2021_alphabet_annual_report.pdf?cache=3a96f54>; ‘Alphabet Year in Review 2020’ (Alphabet, 2021), p. 32 <https://abc.xyz/investor/static/pdf/2020_alphabet_annual_report.pdf?cache=8e972d2>.

³⁶ Calculation based on revenue reported in Alphabet annual reports: ‘Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2018’ (2018) <<https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm>>; ‘Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2019’ (2019) <https://abc.xyz/investor/static/pdf/2019_alphabet_annual_report.pdf?cache=c3a4858>; ‘Alphabet Year in Review 2020’ (Alphabet, 2020) <https://abc.xyz/investor/static/pdf/2020_alphabet_annual_report.pdf?cache=8e972d2>; ‘Alphabet Annual Report 2021’ (Alphabet, 2021) <https://abc.xyz/investor/static/pdf/2021_alphabet_annual_report.pdf?cache=3a96f54>.

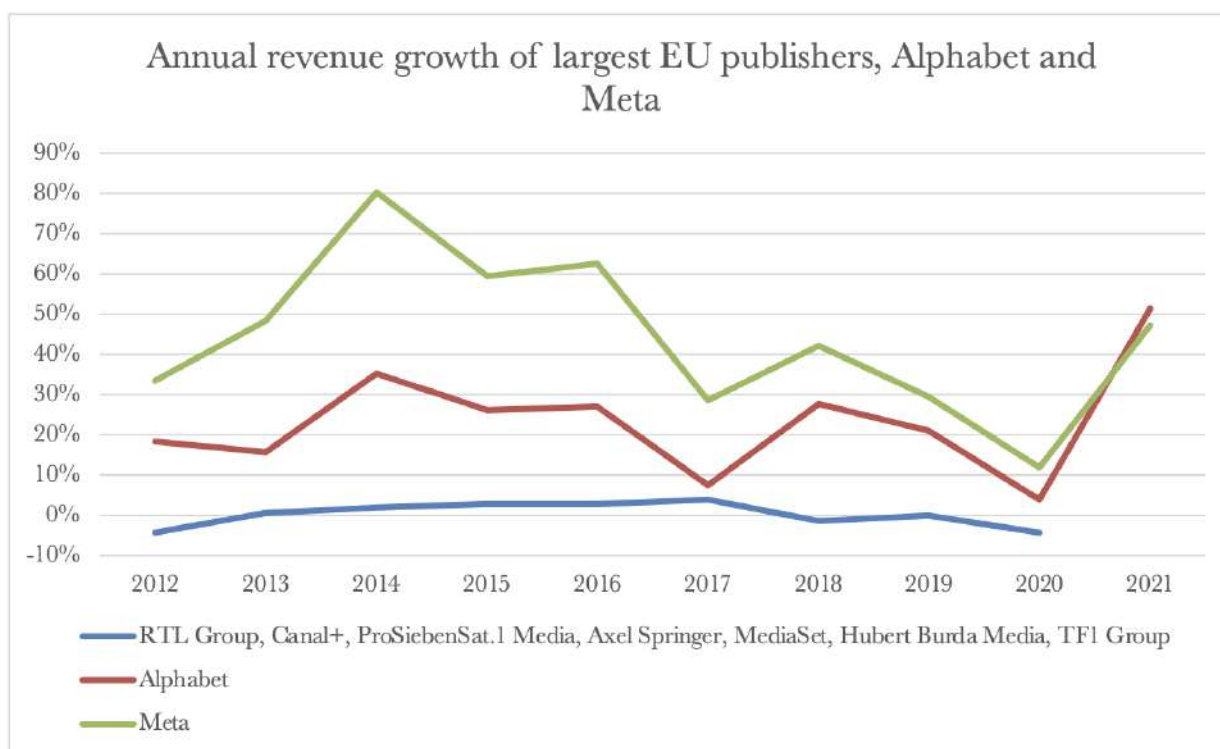


Figure 4: Annual revenue growth of the seven largest EU publishers, Alphabet and Meta. RAI and Bauer Media Group excluded from top EU publishers because of lack of available revenue data. Source: company annual reports and various media coverage.

Google and Meta earn advertising revenue both as publishers and providers of advertising technology services (intermediaries) in the programmatic supply chain. Google generates digital advertising revenues as a publisher through services such as YouTube, Google Maps and Gmail, and Meta does so primarily through Instagram and Facebook. Google and Meta’s intermediary services are described in sections 1.2.2.4 and 1.3.1. Intermediary services can typically charge a fee of up to 12% of the cost of an ad impression³⁷. However, neither company publishes data about how much advertising revenue they earn as publishers compared to as intermediaries. This is why this study will refer to Google and Meta separately as “large platforms”.

Although most publishers do not publish specific data on their revenue from digital advertising in the EEA, below we show the reported advertising revenues of Google and Meta in Europe, the Middle East and Africa (EMEA) and the total global

³⁷ Sources: ‘Guide to Programmatic Media (2014)’ (World Federation of Advertisers, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>> accessed 10 June 2022; Programmatic: Seeing Through the Financial Fog’ (Association of National Advertisers (ANA), May 2017) <<https://www.ana.net/miccontent/show/id/ii-programmatic-financial-fog>> accessed 12 July 2022; ‘ISBA Programmatic Supply Chain Transparency Study’ (ISBA 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

revenues of the 12 biggest publishers with headquarters based in the EEA³⁸ in 2020. That year, Alphabet's total estimated advertising revenue in EMEA amounted to 15% more than the global revenue of the EU's 12 largest publishers combined.

- Alphabet (US), €36.1 billion³⁹
- Meta (US), €16.6 billion⁴⁰
- RTL Group (Germany), €6 billion⁴¹
- Canal+ (France), €5.5 billion⁴²
- ProSiebenSat.1 Media (Germany), €4.05 billion⁴³
- Axel Springer (Germany), €3.11 billion⁴⁴
- Hubert Burda Media (Germany), €2.78 billion⁴⁵
- Mediaset (Italy), €2.64 billion⁴⁶

³⁸ Lack of available data means it was not possible to directly compare the EEA digital advertising revenues of Meta and Google with those of the EEA's largest publishers. As such, the information listed on this page is a comparison of Alphabet and Meta's estimated digital advertising revenues in EMEA (based on our calculation which includes revenues generated from intermediary services) with the EEA's largest publishers' global revenues (including revenue from digital advertising, traditional advertising, subscriptions and distribution).

³⁹ Alphabet's total global revenue in 2020 was €149.7 billion, with EMEA representing 30%. Alphabet reported €120.4 billion of global digital advertising revenue in 2020 but did not provide a breakdown at EMEA level. We have calculated an approximation of Alphabet's EMEA advertising revenue based on 30% of the global figure, although in reality this is likely to be higher given that the EU represents large digital advertising markets. This includes advertising revenues generated both from the placement of ads on the company's owned properties (e.g. YouTube) and revenues from its intermediary services (e.g. Google Ads). 'Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2021' (*Alphabet*, 2021)

<https://abc.xyz/investor/static/pdf/20220202_alphabet_10K.pdf?cache=fc81690>.

⁴⁰ Facebook's total global revenue in 2020 was €70.5 billion, 99.3% of which was digital advertising revenue. Meta reported generating €16.7 billion in revenue in Europe (EU, Russia and Turkey), but did not provide a breakdown of how much of this was advertising revenue. We have calculated an approximation of Meta's digital advertising revenue in Europe based on the 99.3% global figure, although in reality this is likely to be higher given that the EU represents large digital advertising markets. This includes the digital advertising revenues generated both from the placement of ads on the company's publisher platforms (e.g. Instagram) and revenues from its intermediary services (e.g. Meta Audience Network). 'Meta - Financials' (*Meta*)

<<https://investor.fb.com/financials/default.aspx>> accessed 12 May 2022.

⁴¹ 'Annual Report 2020' (*RTL Group*) <<https://www.rtlgroup.com/files/pdf3/rtl-group---annual-report-2020.pdf>>.

⁴² 'Annual Report - Universal Registration Document 2020' (*Vivendi*)

<<https://www.vivendi.com/en/publication/annual-report-universal-registration-document-2020/>> accessed 12 May 2022.

⁴³ 'Annual Report 2020 - Speeding Up' (*ProSiebenSat.1 Media SE*) <<https://annual-report2020.prosiebensat1.com/servicepages/downloads/files/entire-p7s1-ar20.pdf>>.

⁴⁴ 'Axel Springer CFO Expects Double-Digit Sales Growth in 2021 despite Pandemic' (*Reuters*, 14 December 2021) <<https://www.reuters.com/markets/europe/axel-springer-cfo-expects-double-digit-sales-growth-2021-despite-pandemic-2021-12-14/>> accessed 12 July 2022.

⁴⁵ 'Hubert Burda Media - Key Figures' (*Hubert Burda Media*, 2020)

<<https://www.burda.com/en/company/figures/>> accessed 12 July 2022.

⁴⁶ 'Annual Report 2020' (*Mediaset Group*)

<https://www.mfemediaforeurope.com/binary/documentRepository/42/Mediaset%20Group%20-%20Annual%20Report%202020_1519.pdf>.

- RAI (Italy), €2.36 billion⁴⁷
- Bauer Media Group (Germany), €2.30 billion⁴⁸
- TF1 Group (France), €2.08 billion⁴⁹
- Ströer (Germany), €1.44 billion⁵⁰
- Schibsted Media Group (Norway), €1.29 billion⁵¹
- PRISA (Spain), €1.10 billion⁵²

The revenues of some of the largest EU publishers have stagnated over the past ten years (see Figure 4). The combined revenues of RTL Group (Germany)⁵³, Canal+ (France)⁵⁴, ProSiebenSat.1 Media (Germany)⁵⁵, Axel Springer (Germany)⁵⁶, Mediaset (Italy)⁵⁷, Hubert Burda Media (Germany)⁵⁸ and TF1 Group (France)⁵⁹ were €25.61 billion in 2011. By 2020, they had grown slightly to €26.04 billion (see list above), an increase of just 1.67%. Between 2012 and 2020, their combined annual revenue growth remained under 5%, and contracted on three occasions.

During this period Alphabet and Meta's global revenues increased significantly and both companies saw double-digit growth almost every year. From 2020 to 2021, Alphabet and Meta's revenues increased 51% and 57% respectively.

⁴⁷ 'Report and Financial Statements as at 31 December 2021' (Rai)

<https://www.rai.it/dl/doc/1632746560527_UK%20Rai%20RFA%202020.pdf>.

⁴⁸ 'Bauer Media Group (Hamburg): Umsatz, Mitarbeiterzahl' (Die Deutsche Wirtschaft)

<https://die-deutsche-wirtschaft.de/famu_top/bauer-media-group-hamburg-umsatz-mitarbeiterzahl/> accessed 12 July 2022.

⁴⁹ 'Management Report 2021' (Groupe TF1) <https://groupe-tf1.fr/sites/default/files/pdf-financiers/management_report_tf1_2021_eng_-_vdef.pdf>.

⁵⁰ 'Financial Reports' (Ströer SE) <<https://ir.stroeer.com/investor-relations/financial-reports/>> accessed 12 July 2022.

⁵¹ 'Reports & Presentations' (Schibsted) <<https://schibsted.com/ir/reports-presentations-calendar/>> accessed 12 July 2022.

⁵² 'Promotora de Informaciones, S.A. - Financial Statements and Management Report for the Year Ended December 31, 2020' (Prisa) <https://www.prisa.com/uploads/2021/03/financial-statements-stand-alone-prisa-311220pdf_1.pdf>.

⁵³ '2011 Annual report' (RTL Group)

<https://www.annualreports.com/HostedData/AnnualReportArchive/r/rtl-group_2011.pdf>.

⁵⁴ '2011 Annual Report (Vivendi) <https://www.vivendi.com/wp-content/uploads/2013/04/20120330_Annual_Report_2011-2.pdf>

⁵⁵ 'Annual Report 2011' (ProSiebenSat.1 Group) <<http://prosiebensat1.corporate-reports.net/prosiebensat1/annual/2011/gb//English/pdf/report.pdf>>.

⁵⁶ 'Annual Report 2011' (Axel Springer AG)

<https://www.axelspringer.com/data/uploads/2021/11/Annual-Report-2011_Axel-Springer-AG.pdf>.

⁵⁷ 'Bilancio 2011' (Mediaset)

<https://www.mfemediaforeurope.com/binary/documentRepository/48/FY2011_Annual_report_IT_A_804.pdf>.

⁵⁸ 'Annual Report 2011' (Hubert Burda Media)

<https://issuu.com/burda_news/docs/media_in_transition_2012/161>.

⁵⁹ 'Financial Report 2011' (TF1) <https://groupe-tf1.fr/sites/default/files/tf1_2011_activity_report.pdf>.

1.2.2.1.1 Comparison of the revenues of publishers and large platforms

The large gap in revenue between Google and Meta on the one hand, and European publishers on the other is partly a matter of scale. Before the internet, the media landscape was fragmented. Advertisers needed to split their advertising spend across a large range of smaller, more localised media outlets, such as TV channels, radio stations, newspapers, billboards and magazines, in order to reach a large number of people across geographies. Google and Meta, however, provide a service to billions of people across locations, languages and cultural contexts in a way that traditional, offline media outlets were not designed to do. From an advertising perspective, this has changed the scale of reach that a single ad placed on a single channel can achieve. This has proved attractive to advertisers, particularly the large global corporations that make up a significant part of global ad spend⁶⁰. Both large and small advertisers interviewed for this study explained that a primary motivation for advertising with Google and Meta was being able to reach a large number of people with their advertising messages. Reaching the equivalent number of people via news publishers was seen as requiring significantly more effort and investment in resources at the local level, due to the smaller audiences split across a large number of publishers in different countries.

Advertising spend also tends to flow to places where consumers spend time. Since 2011, the number of people using services and platforms provided by Google and Meta has increased significantly. Daily Google searches have increased by 63% (from 5.5 billion in 2011⁶¹ to 8.5 billion in 2021)⁶², and Facebook users have tripled (from 484 million in 2011 to 1.929 billion)⁶³. The rapid growth of social media advertising is linked to this increase, while display advertising on publisher channels has declined. Meta and Google have remained the key players linking an increase in time spent on their platforms to advertising revenue, even though other players have been emerging. TikTok reached one billion users after only four years, compared to Facebook, YouTube and Instagram which took eight years to

⁶⁰ The 30 biggest advertisers make up 32% of global ad spend. 'Spotlight #5 - Top 30 Global Advertisers 2020' (*COMvergence*, May 2021) <<https://comvergence.net/wp-content/uploads/2021/10/comvergence-spotlight-may-2021-5501.pdf>>; 'Advertising Expenditure Forecasts December 2021' (*Zenith*, December 2021) <https://s3.amazonaws.com/media.mediapost.com/uploads/Advertising_Expenditure_Forecasts_December_2021_0N69DuK.pdf>.

⁶¹ Dopico A, 'How Many Google Searches Were There in 2011?' (*janetpanic.com*, 30 May 2019) <<https://janetpanic.com/how-many-google-searches-were-there-in-2011/>> accessed 7 June 2022.

⁶² Mohsin M, '10 Google Search Statistics You Need to Know in 2022' (*Oberlo*, 2 January 2022) <<https://www.oberlo.com/blog/google-search-statistics>> accessed 7 June 2022.

⁶³ 'Facebook: Daily Active Users Worldwide 2021' (*Statista*) <<https://www.statista.com/statistics/346167/facebook-global-dau/>> accessed 13 June 2022.

reach the same milestone⁶⁴. In China, Douyin (an app owned by the same parent company as TikTok) now accounts for 12% of total time spent online⁶⁵.

As more time is spent in these online environments, people's attention can be transformed into profit through advertising. Alphabet links its growth directly to this factor: "The continuing shift from an offline to online world has contributed to the growth of our business since inception, contributing to revenue growth, and we expect that this online shift will continue to benefit our business"⁶⁶. Although many publishers have innovated to provide new services and content to users, they have struggled to compete with the network effects of social media and other large platforms.

Meanwhile, search has created an entirely new channel for advertising. Rather than monetising people's attention, search advertising is able to monetise signals about people's intent. Search platforms are also expanding to provide news and information content to users within their own ecosystems, which enables them to compete with social media and publishers for attention-based advertising revenue⁶⁷. This has diversified the competitive landscape of digital advertising, creating new opportunities for advertisers while potentially limiting publishers' ability to play as central a role as they did in traditional offline environments.

The role of the "ecosystem" is important for advertising revenue. As well as providing a platform for ads to be displayed, companies are incentivised to keep people within their "owned-and-operated" ecosystems in order to observe their behaviour and collect data that can be used to increase the value of advertising shown to them. Advertisers are willing to pay significantly more to show advertising to people who they know are interested in the product, although the available evidence varies as to how much⁶⁸. A 2019 US study found that advertisers are willing to spend 63% more on average for some form of targeting for their ads⁶⁹. Although the ability to collect this data using third-party cookies and trackers was open to hundreds, if not thousands, of companies in the past, in

⁶⁴ 'The All-Conquering Quaver' (*The Economist*, 2022) <<https://www.economist.com/interactive/briefing/2022/07/09/the-all-conquering-quaver>> accessed 19 July 2022.

⁶⁵ 'The All-Conquering Quaver' (*The Economist*, 2022) <<https://www.economist.com/interactive/briefing/2022/07/09/the-all-conquering-quaver>> accessed 19 July 2022.

⁶⁶ 'Alphabet Inc. Form 10-K for the Fiscal Year Ended December 31, 2019' (2019) <https://abc.xyz/investor/static/pdf/2019_alphabet_annual_report.pdf?cache=c3a4858>.

⁶⁷ 'Google Benefit from News Content – Economic Study' (*News Media Alliance*, June 2019) <<http://www.newsmediaalliance.org/wp-content/uploads/2019/06/Google-Benefit-from-News-Content.pdf>>.

⁶⁸ See section 2.4.

⁶⁹ Marotta V, Abhishek V and Acquisti A, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (2019) <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>.

the future it is likely that only companies who own and operate the ecosystems where people spend time will be able to do this⁷⁰. While most publishers' ecosystems are limited to a small number of websites and apps (or, in the case of small publishers, just one website or one app), platforms like Google can collect data from an extensive network of owned-and-operated services including Europe's biggest browsers and operating systems, as well as some of the most widely used websites and apps in the world.

1.2.2.2 Advertisers

Advertisers are entities that advertise via the digital advertising channels described in section 1.1.2. The biggest 30 advertisers together represented 32% of global advertising spend (€119 billion) in 2020. Each of these 30 companies spent at least €1 billion on advertising in 2020, 25-50% of which was spent on digital advertising⁷¹.

The ten biggest advertisers by advertising spend globally are Procter & Gamble (1.3% of total global ad spend), Unilever (0.7%), L'Oréal (0.5%), Amazon (0.4%), Nestlé (0.4%), Volkswagen (0.4%), Renault-Nissan-Mitsubishi Alliance (0.4%), Stellantis (0.4%), General Motors Company (0.3%) and Reckitt Benckiser Group (0.3%)⁷². Three of these companies are headquartered in EU Member States (France, Germany, the Netherlands), one is in Switzerland and two are in the UK.

1.2.2.3 Media agencies

Some large advertisers use media agencies to advise them on how and where to promote their products through traditional and digital advertising channels. The largest media agencies globally are GroupM (15.5% market share), Publicis Groupe (10.7%) and Omnicom Media Group Holdings (9.8%)⁷³. Media agencies typically operate Agency Trading Desks (ATDs) to manage the buying and placement of ads in digital channels programmatically.

⁷⁰ See section 1.3.1.2.

⁷¹ 'Spotlight #5 - Top 30 Global Advertisers 2020' (COMvergence, May 2021) <<https://comvergence.net/wp-content/uploads/2021/10/comvergence-spotlight-may-2021-5501.pdf>>.

⁷² 'Spotlight #5 - Top 30 Global Advertisers 2020' (COMvergence, May 2021) <<https://comvergence.net/wp-content/uploads/2021/10/comvergence-spotlight-may-2021-5501.pdf>>.

⁷³ 'Exclusive Data from COMvergence on Media Agency Billings Final 2020 Reveals Top Global Agency Network and Group Winner' (GroupM, 26 July 2021) <<https://www.groupm.com/newsroom/exclusive-data-from-comvergence-on-media-agency-billings-final-2020-reveals-top-global-agency-network-and-group-winner/>> accessed 12 June 2022.

1.2.2.4 Intermediaries

Advertisers and publishers, especially large ones, often work with a range of intermediaries to buy and sell advertising through different channels. These intermediaries are sometimes referred to as “ad tech” companies. There are two key categories of intermediaries:

- 1) Programmatic intermediaries that perform specific functions to enable ads to be bought and sold programmatically⁷⁴. This includes DSPs, SSPs, ad exchanges, and data management platforms (DMPs).
- 2) Verification providers, which are used by advertisers (often large ones) to assess that their digital advertising meets certain standards across various different channels and platforms. This can include viewability (how much of an ad was seen and for how long), brand safety (assessing the context in which ads are placed) and fraud (ensuring that ads are not seen or clicked by bots instead of humans).

In the US, the Texas Attorney General has noted Google as having “monopoly power” in the categories of DSPs, SSPs and ad exchanges, describing the company as “pitcher, batter and umpire” in the programmatic display advertising market⁷⁵.

1.2.2.4.1 Demand-side Platforms

Demand-side platforms (DSPs) enable advertisers and agencies to automate the buying of digital advertising from many sources. Industry studies estimate that DSP fees amount to approximately 8-12% of programmatic ad spend⁷⁶, which could amount to up to €2.5-3.8 billion in the EEA⁷⁷.

⁷⁴ See section 1.1.2.4 for more detail on how programmatic advertising works.

⁷⁵ *The State of Texas, et al v Google LLC* [2020] (United States District Court, Eastern District of Texas, Sherman Division), <https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216%20COMPLAINT_REDACTED.pdf>.

⁷⁶ ‘Guide to Programmatic Media (2014)’ (*World Federation of Advertisers*, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>> accessed 5 June 2022; Programmatic: Seeing Through the Financial Fog’ (*Association of National Advertisers*, May 2017) <<https://www.ana.net/miccontent/show/id/ii-programmatic-financial-fog>> accessed 26 July 2022; ‘ISBA Programmatic Supply Chain Transparency Study’ (*ISBA*, 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁷⁷ Approximately €46 billion was spent on digital advertising in the EEA in 2021. Based on industry forecasts for 19 EEA Member States, we have estimated that about 61% of that spend was bought programmatically in 2021, or approximately €28 billion. Austin A, Barnard J and Hutcheon N, ‘Programmatic Marketing Forecasts’ (*Zenith*, 2019) <<https://s3.amazonaws.com/media.mediapost.com/uploads/ProgrammaticMarketingForecasts2019.pdf>>; and WPP (December 2021).

Spain (2019)⁷⁸	UK (2019)⁷⁹	Australia (2020)⁸⁰
Google (DV360): >60% The Trade Desk: <20% Amazon: <20% Adobe: <10% Xandr-AppNexus: <5% MediaMath: <5% Verizon: <5% Sonata-TapTap: <5% Other: <5%	Google (Google Ads and DV360): 40-60% The Trade Desk: 0-10% Xandr-AppNexus: 0-10% Criteo: 0-10% Amazon DSP: 0-10% Others: 0-10%	Google: 60-70%

Table 2: Revenue market shares of the largest DSPs in Spain, the UK and Australia according to calculations done by local competition authorities. Some of these companies may have changed name and/or ownership since these calculations were published.

Table 2 provides an overview of the estimated revenue market shares of the largest DSPs in Spain, the UK and Australia according to calculations done by the local competition authorities. In all three countries, competition authorities found that Google services, including Display & Video 360 and Google Ads, held high market shares. All DSPs listed in table 2 are owned by companies with headquarters in the US, with the exception of Adform (based in Denmark), TapTap (based in Spain) and Criteo (based in France).

1.2.2.4.2 Supply-side Platforms

Supply-side platforms (SSPs) are used by publishers to manage, sell and optimise advertising space (also known as ad inventory) on their websites, mobile apps and other digital properties in an automated way. SSPs enable publishers to connect their ad inventories to multiple ad exchanges and DSPs. SSPs today also typically perform functions which used to sit separately under “ad exchanges”, namely facilitating the buying and selling of advertising inventory using auction-based systems to determine the price of inventory according to parameters set by publishers and advertisers.

⁷⁸ ‘E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain’ (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

⁷⁹ ‘Online Platforms and Digital Advertising - Market Study Final Report’ (Competition and Markets Authority, 2020), p.19 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

⁸⁰ ‘Digital Advertising Services Inquiry Final Report’ (Australian Competition and Consumer Authority, 2021) <<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

Spain (2019)⁸¹	UK (2019)⁸²	Australia (2020)⁸³
Google (AdX): >50%	Google (AdX): 50-60%	Google: 40-50%
Teads: <10%	Xandr-AppNexus: 10-20%	
Xandr-AppNexus: <10%	Magnite-Rubicon: 0-10%	
Magnite-Rubicon: <10%	Others: 10-20%	
Smart AdServer: <10%		
Rich Audience: <10%		
Verizon: <10%		
SpotX: <10%		
SunMedia: <10%		
Adman: <10%		
Seedtag: <5%		
Index Exchange: <5%		
FreeWheel-Comcast: <5%		
OpenX: <5%		
Other: <5%		

Table 3: Revenue market share of the largest SSPs in Spain, the UK and Australia according to calculations done by local competition authorities. Some of these companies may have changed name and/or ownership since these calculations were published.

Industry studies estimate that SSP fees amount to approximately 8% of programmatic ad spend⁸⁴, which could amount to up to €2.5 billion in the EEA⁸⁵.

Table 3 provides an overview of the estimated revenue market share of the largest SSPs in Spain, the UK and Australia according to calculations done by local competition authorities. In all three countries, competition authorities found that Google held the largest market share. All SSPs listed in table 3 are owned by companies with headquarters in the US, with the exception of Smart AdServer (based in France), Rich Audience (based in Spain), SunMedia (based in Spain), Adman (based in Greece), and Seedtag (based in Spain).

⁸¹ 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

⁸² 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p.19 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

⁸³ 'Digital Advertising Services Inquiry Final Report' (Australian Competition and Consumer Authority, 2021) <<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

⁸⁴ 'ISBA Programmatic Supply Chain Transparency Study' (ISBA, 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁸⁵ See footnote 77.

1.2.2.4.3 Ad servers

An ad server is a web server that hosts information about ads and delivers advertising content to different digital platforms, websites and mobile apps. Ad servers place ads within ad inventory and target audiences according to advertisers' criteria. Ad servers can also track impressions delivered and the performance of ads, and help with the management and optimisation of campaigns. There are two types of ad servers:

- **Publisher ad servers:** used by publishers to serve and manage ads within their own inventory. Publishers use them to set the decision logic underlying the ads served on their inventory based on bids they receive from SSPs and through direct deals with advertisers. This involves defining the priorities according to which ads should be placed on a publisher's inventory (e.g. pricing and demand sources). The CMA estimates that publisher ad server fees amount to approximately 0-5% of programmatic ad spend⁸⁶, which could amount to up to €1.6 billion in the EEA⁸⁷.
- **Advertiser ad servers:** used by advertisers to run campaigns, manage their "creative" (i.e. the content of the ad), and track and analyse the performance of ads delivered. Similarly to publisher ad servers, they are used to collect various measurement data associated with campaigns (e.g. clicks, impressions). Additionally, they can be used to optimise campaigns through methods such as "A/B testing", which test the performance of campaigns under different scenarios (e.g. different targeting criteria). They are also used to set the frequency associated with ads (i.e. the maximum number of times a user should see an ad). The CMA estimates that publisher ad server fees amount to approximately 3% of programmatic ad spend⁸⁸, which could amount to up to €1 billion in the EEA⁸⁹.

Tables 4 and 5 provide an overview of the estimated revenue market shares of the largest publisher ad servers and advertiser ad servers in Spain, the UK and Australia according to calculations done by the local competition authorities. The competition authorities found that Google held the largest market share. All ad servers listed in tables 4 and 5 are owned by companies with headquarters in the US, with the exception of Smart AdServer (based in France), Weborama (based in France) and Adform (based in Denmark).

⁸⁶ 'Appendix R: Fees in the Adtech Stack', in 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020) <https://assets.publishing.service.gov.uk/media/5fe49625e90e071207e10eff/Appendix_R_-_fees_in_the_adtech_stack_WEB.pdf> .

⁸⁷ See footnote 77.

⁸⁸ 'Appendix R: Fees in the Adtech Stack', in 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020) <https://assets.publishing.service.gov.uk/media/5fe49625e90e071207e10eff/Appendix_R_-_fees_in_the_adtech_stack_WEB.pdf> .

⁸⁹ See footnote 77.

Spain (2019)⁹⁰	UK (2019)⁹¹	Australia (2020)⁹²
Google: >70% Smart AdServer: <20% FreeWheel-Comcast: <10% Xandr-AppNexus: <5% Other: <5%	Google Ad Manager: 90-100% FreeWheel-Comcast: 0-10% Verizon Media: 0-10% Smart AdServer: 0-10%	Google: 90-100%

Table 4: Revenue market shares of the largest publisher ad servers in Spain, the UK and Australia according to calculations carried out by local competition authorities. Some of these companies may have changed name and/or ownership since these calculations were published.

Spain (2019)⁹³	UK (2019)⁹⁴	Australia (2020)⁹⁵
Google: >70% Sizmek-Amazon: <20% Weborama: <10% Adform: <5% Flashtalking: <5% Innovid: <5% Other: <5%	Google: 80-90% Flashtalking: 10-20% Sizmek-Amazon: 0-10% Adform: 0-10% Innovid: 0-10%	Google: 80-90%

Table 5: Revenue market shares of the largest advertiser ad servers in Spain, the UK and Australia according to calculations carried out by local competition authorities. Some of these companies may have changed name and/or ownership since these calculations were published.

⁹⁰ 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

⁹¹ 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p.19 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

⁹² 'Digital Advertising Services Inquiry Final Report' (Australian Competition and Consumer Authority, 2021) <<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

⁹³ 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

⁹⁴ 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p.19 <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

⁹⁵ 'Digital Advertising Services Inquiry Final Report' (Australian Competition and Consumer Authority, 2021) <<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

1.2.2.4.4 Ad exchanges

Ad exchanges are platforms that facilitate the buying and selling of advertising inventory using real-time bidding to determine the price of inventory according to the parameters set by both publishers and advertisers. Ad exchanges match transactions between DSPs and SSPs. Today, the functions of ad exchanges are largely undertaken by SSPs. In the past, ad exchanges used to be platforms that were separate from SSPs. Industry studies estimate that exchange fees can amount to up to 5% of programmatic ad spend⁹⁶.

1.2.2.4.5 Data Management Platforms

Data management platforms (DMPs) allow advertisers, DSPs, SSPs and publishers to manage and analyse their data, combine it with data provided by third parties, and create audiences that can be used for digital advertising based on profiling. Digital advertising based on profiling enables advertisers to target ads to people based on data gathered about their online behaviour, preferences, location and demographic information. Other data can also be used to target ads, such as information about the content being viewed, the device being used and location. This data can be provided by publishers when they make the ad space available in the programmatic system. Advertisers can also match data they have about individuals with the data being shared by publishers in order to target (or exclude) specific users with (or from) advertising. Some DMPs also integrate data from other second- and third-party data sources, such as data brokers. DMPs also make this data available to other platforms, including DSPs, SSPs and ad exchanges.

1.2.2.4.6 Ad networks

Advertisers and publishers use ad networks to buy and sell display advertising (respectively). Ad networks can purchase ad inventory at a fixed price from publishers and sell it on to advertisers or do so using real-time bidding. Some ad networks may also buy inventory from SSPs and sell inventory to DSPs.

1.2.2.4.7 Verification

Verification tools offer services that claim to help advertisers tackle a number of challenges related to digital advertising including brand safety, viewability and ad fraud. These tools can be made available on the advertiser (demand) side as well as the publisher (supply) side. Industry estimates indicate that verification companies can receive up to 25% of ad spend in exchange for their services⁹⁷.

⁹⁶ 'Guide to Programmatic Media (2014)' (*World Federation of Advertisers*, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>> accessed 15 May 2022.

⁹⁷ Sources: 'Guide to Programmatic Media (2014)' (*World Federation of Advertisers*, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>> accessed

a) Brand safety

Brand safety tools claim to enable advertisers to have more control over where their ads are placed: they can exclude specific publisher sites (exclusion lists), restrict ad placements to specific publisher sites indicated by the advertiser or agency (inclusion lists), exclude (or include) only certain types or categories of publisher based on a range of criteria, and exclude (or include) certain types of content based on criteria such as keywords and categories. These tools have become increasingly popular among advertisers in response to a number of investigations that have shown advertising (often bought programmatically) appearing next to terrorist content⁹⁸, explicit conversations about sexual abuse of children⁹⁹, climate change denial¹⁰⁰ and hate speech¹⁰¹ (see also section 2.2.1.2).

b) Viewability

Viewability is a term used to describe whether or not an ad “ever appeared in the space within a webpage that was in view to the viewer”¹⁰². Viewability tools are used to ensure that ads which are never seen by a human (e.g. because they appear at the bottom of a webpage and the user did not scroll down far enough to see it) are not paid for, based on industry standards¹⁰³.

c) Ad fraud

Some verification tools claim to be able to identify fraudulent activity designed to capture advertising revenue, such as bots that artificially inflate the number of ad impressions or clicks (known as “invalid traffic”). The Advertising Fraud Council suggests that the parties responsible for ad fraud generally fall into four categories: “black hat” marketers, fraudulent ad networks, common

8 June 2022; Programmatic: Seeing Through the Financial Fog’ (*Association of National Advertisers*, May 2017) <<https://www.ana.net/miccontent/show/id/ii-programmatic-financial-fog>> accessed 8 June 2022; ‘ISBA Programmatic Supply Chain Transparency Study’ (*ISBA*, 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁹⁸ Mostrous A, ‘Big Brands Fund Terror through Online Adverts’ (*The Times*, 9 February 2017) <<https://www.thetimes.co.uk/article/big-brands-fund-terror-knnxfgb98>> accessed 29 July 2022.

⁹⁹ Murphy H, ‘Companies Pull YouTube Advertising over Child Exploitation Fears’ (*Financial Times*, 21 February 2019) <<https://www.ft.com/content/2087c944-3584-11e9-bb0c-42459962a812>> accessed 3 June 2022.

¹⁰⁰ ‘Why Is YouTube Broadcasting Climate Misinformation to Millions?’ (*Avaaz*, 16 January 2020) <https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/>.

¹⁰¹ ‘Home’ (*Stop Hate for Profit*) <<https://www.stophateforprofit.org>> accessed 29 August 2022.

¹⁰² ‘Glossary of Terminology’ (*IAB*) <<https://www.iab.com/insights/glossary-of-terminology/>> accessed 7 August 2022.

¹⁰³ ‘MRC Viewable Impression Guidelines’ (*IAB*) <<https://www.iab.com/guidelines/mrc-viewable-impimpression-guidelines/>> accessed 7 August 2022.

cybercriminals and organised criminals¹⁰⁴. However, identifying the parties responsible for ad fraud is challenging, given both the illegality of certain practices and the existing lack of transparency within the supply chain¹⁰⁵.

1.3 Overview of the role and value of data in digital advertising, how this is evolving in light of recent developments and how this is communicated to users

1.3.1 Overview of the role and value of data in digital advertising and how this is evolving in light of recent developments

The most widely used products in the digital advertising market rely on large amounts of personal data and profiling of individuals. Large platforms control access to a significant proportion of the personal data that is used for digital advertising. Their use of this data is often opaque to individuals, the companies who depend on them and regulators. Some of these platforms are taking steps to limit other companies' access to data generated through the use of their operating systems and services, often citing privacy and data protection as a key motivating factor.

This section describes the different ways in which data is collected for digital advertising, how users are identified, the types of data (including personal data) that are collected, and the perceived value that is derived from this data¹⁰⁶.

1.3.1.1 Role of identifiers

Identifiers that can connect data from different sources to an individual are a central part of digital advertising today. Identifiers can take many forms, including cookie IDs, mobile advertising IDs and internet protocol (IP) addresses. Because many of these IDs are specific to just one device, the advertising industry has

¹⁰⁴ Kotila M, Rumin RC and Dhar S, 'Compendium of Ad Fraud Knowledge for Media Investors' (*World Federation of Advertisers & The Advertising Fraud Council*, 2016) <<https://swa-asa.ch/wAssets/docs/publikationen/de/branchenempfehlungen-swa/WFACompendiumofAdFraudKnowledge.pdf>>.

¹⁰⁵ 'Integral Ad Science | Protect Your Ads from Fraud' (*Integral Ad Science*) <<https://integralads.com/solutions/ad-fraud/>> accessed 7 August 2022.

¹⁰⁶ Contributions to this section were provided by Alan Toner.

developed techniques to identify and connect IDs across multiple devices. Techniques such as “identity graphs” are used to connect data from different sources to create a view of an individual’s activity across devices and services, using “join keys” – a shared dimension between two data records that allows them to be connected. Accuracy in identification techniques relies on the robustness of the join key and ranges from deterministic (strong) to probabilistic (weak).

Online identifiers are mentioned in the General Data Protection Regulation’s (GDPR) definition of personal data¹⁰⁷. Recital 30 GDPR notes that “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them”¹⁰⁸. Typically though, digital advertising identifiers are not used to target ads at an individual level (even if this may be technically possible – see section 2). Rather, identifiers are used to attach certain characteristics to an individual so that they can be grouped together with other individuals that share similar characteristics. Advertisers and their agencies can then target ads to these groups (often called “segments”).

This section will describe the types of data collected (e.g. demographic, interests, intent, location) as part of digital advertising. That said, in reality, different types of data are usually combined using identifiers to create profiles and categorise users into “segments” that ads can be targeted towards (e.g. women aged 20-30 in Paris with pets). This can be done through a variety of different actors using different means.

The perceived value of data in the digital advertising industry tends to be cumulative. Additional data points about an individual are considered as building a deeper understanding of their interests or intent, enabling more accurate targeting and more successful outcomes for the ads shown to them. Identifiers that enable individuals to be tracked as they move across platforms and devices are important in order to build profiles of individuals based on multiple data points.

¹⁰⁷ Under Article 4.1 GDPR, personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier.” *EU The General Data Protection Regulation (GDPR): 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)*, OJ 2016 L 119/1.

¹⁰⁸ *EU General Data Protection Regulation (GDPR): 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)*, OJ 2016 L 119/1.

This is why market and regulatory shifts that affect the ability of some actors to connect data to identifiers (e.g. Google's Privacy Sandbox) are considered so significant for the industry (see section 1.3.1.2).

There are four main ways of identifying users in the digital advertising ecosystem today: cookie IDs, mobile IDs, fingerprinting and user IDs. Identifiers across all four categories can be combined to reveal additional information about individuals.

1.3.1.1.1 Cookie IDs

Cookies and pixels have, until now, been the most common means of tracking interaction in the absence of a verified user account¹⁰⁹. Recital 25 of Directive 2002/58/EC (the ePrivacy Directive)¹¹⁰ states that cookies "can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in online transactions"¹¹¹. The ePrivacy Directive also provides that cookies may only be deployed with the consent of the individual user, except where they are necessary for the purpose of carrying out electronic communications, or where they are necessary in order to provide a service they have explicitly requested¹¹².

Cookies are set by a server via HTTP, or through JavaScript on the client side, and are stored in the user's browser. "Cookie syncing" enables the data collected by

¹⁰⁹ See section 1.3.1.1.4 for a more detailed explanation of user IDs in advertising.

¹¹⁰ 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), OJ L 201, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>.

¹¹¹ 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), OJ L 201, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>.

¹¹² Article 5.3 ePrivacy Directive states that "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." Additionally, Recital 25 states that "users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment." 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), OJ L 201, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>.

cookies to be consolidated and linked to central identifiers, which are used for advertising purposes. The result of the sync is a matching table entry where the identifiers used by different companies for the same user are reconciled¹¹³ (e.g. SharedID managed by Prebid and Unified ID 1.0 managed by The Trade Desk)¹¹⁴.

Cookies can be used to collect data about people's browsing history, including the websites or pages they visit and the content they view. This is often used to infer people's interests, intents, location and demographic data (e.g. age, gender), including categories of personal data such as race, political views, religion and sexual orientation. They are used by a wide range of companies to collect and link data, including Google, Meta, publishers, advertisers and intermediaries.

1.3.1.1.2 Mobile IDs

Mobile devices have unique resettable mobile advertising identifiers (MAIDs), introduced to replace the non-resettable universally unique identifiers (UUIs) used for tracking and advertising in the early period of mobile advertising¹¹⁵, ¹¹⁶. Mobile device identifiers have a stronger association with individuals than computers, as the latter may be used by a household or different members of an organisation.

MAIDs are used to link data collected by an individual's phone to a specific individual. The MAID can then be used to identify, profile and segment people for advertising purposes. Data can be collected at operating system level or by apps.

¹¹³ 'What is Cookie Syncing and How Does it Work?' (*Clearcode*, 7 June 2022) <<https://clearcode.cc/blog/cookie-syncing/>> accessed 19 May 2022. Syncs use different methods. For example, as a page loads, calls are made to advertising services. Domain X is contacted by the user's browser and either returns an existing cookie or sets a new identifier, '789'. To this response, a redirect is added to the other party to the sync. The browser receives cookie '789' then sends it to the other party to the sync, domain 'Y', which has a parallel identifier for the same user, 'abc'. Now 'Y' knows that '789' and 'abc' are the same user and stores the data in the matching table. The two domains can now execute a batch data transfer about relevant users over a server to server connection (not observable through the browser). For an anatomical analysis of a cookie sync, see Christl W, 'Digital Profiling in the Online Gambling Industry' (*Cracked Labs*, 2022) <<https://cdn.sanity.io/files/btrscf0/production/e23ea75fe93f775d9f9ed795427f4b5ed8d67016.pdf>>.

¹¹⁴ Prebid.org is an industry group established to steward open-source technologies. 'Prebid' (*Prebid*) <<https://prebid.org/>> accessed 12 August 2022.

¹¹⁵ Android's Advertising ID was launched in 2014. See: 'Best Practices for Unique Identifiers' (*Android Developers*) <<https://developer.android.com/training/articles/user-data-ids>> accessed 12 June 2022. Apple introduced the ID for Advertisers (IDFA) in 2011.

¹¹⁶ Although the intention behind MAIDs was to transition from non-resettable IDs for privacy reasons, research by Serge Egelman in 2019 found 18,000 apps collecting non-resettable IDs such as IMEI, WiFi MAC addresses, and SIM card serial numbers. See: Sharma S, '18,000 Android Apps Track Users by Violating Advertising ID Policies' (*FOSSBYTES*) <<https://fossbytes.com/android-apps-violating-google-advertising-id-policies/>> accessed 12 April 2022.

MAIDs are specific to the operating system used by the phone. The most prevalent MAIDs in Europe are Google's Advertising ID (GAID) on the Android operating system (used by 69% of mobile devices in Europe in 2022) and Apple's Identifier for Advertisers (IDFA) on the iOS operating system (used by 30% of devices)¹¹⁷. Google, and apps which use its software development kits (SDKs)¹¹⁸, have access to the GAID on all Android devices.

In February 2022, Google announced a plan to phase out the GAID, and replace it with new technologies developed in the context of its Privacy Sandbox initiative on Android (see section 5 for further discussion of Privacy Sandbox)¹¹⁹. Similarly, use of Apple's IDFA is declining since Apple introduced a new framework for app tracking known as App Tracking Transparency (ATT) in early 2021. This framework presents an "app-tracking authorisation request" to users¹²⁰ which, unlike most consent requests for ad tracking, presents "ask app not to track" as the first option (see figure 5). When this consent request was introduced, 89% of users worldwide selected "ask app not to track", thereby preventing their data from being linked to the IDFA¹²¹.

Considering the low opt-in rates on Apple devices, coupled with Google's plans to phase out the GAID, the role of MAIDs in digital advertising could become a lot less significant in the future. Companies that until now have relied heavily on MAIDs for advertising revenue have already reported big losses following Apple's moves¹²².

¹¹⁷ 'Mobile Operating System Market Share Europe' (*StatCounter Global Stats*)

<<https://gs.statcounter.com/os-market-share/mobile/europe>> accessed 7 May 2022.

¹¹⁸ App developers enhance the functionality of their apps through the addition of third-party code, known as software development kits (SDKs) or third-party libraries.

¹¹⁹ Chavez A, 'Introducing the Privacy Sandbox on Android' (*Google*, 16 February 2022)

<<https://blog.google/products/android/introducing-privacy-sandbox-android/>> accessed 12 May 2022.

¹²⁰ 'App Tracking Transparency' (*Apple Developer Documentation*)

<<https://developer.apple.com/documentation/apptrackingtransparency>> accessed 7 May 2022.

¹²¹ Balasubramanian, 'App Tracking Transparency Opt-In Rate - Monthly Updates' (*Flurry*, 18 February 2022) <<https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/>> accessed 7 May 2022.

¹²² For example, Facebook claimed that Apple's ATT changes would lead to losses of €9 billion for the company in 2022. 'Fourth Quarter 2021 Results Conference Call' (*Meta Platforms Inc*, 2 February 2022) <https://s21.q4cdn.com/399680738/files/doc_financials/2021/q4/Meta-Q4-2021-Earnings-Call-Transcript.pdf>.

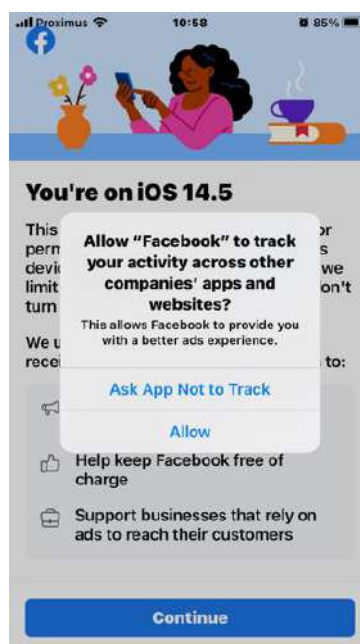


Figure 5: Apple's ATT consent request, presented by the Facebook app. Source: screenshot taken 28 May 2021.

1.3.1.1.3 Fingerprinting

Fingerprints are generated by combining attributes of the user's device or browser with data standardly provided in network requests (e.g. IP address, user agent string, OS version)¹²³. The permutation of these features is used by intermediaries to generate a hash which is used as an identifier and database key for that user¹²⁴. Since first being deployed in 2010, fingerprinting has become increasingly widespread¹²⁵. One estimate suggests that fingerprinting techniques are deployed

¹²³ See Eckersley P, 'How Unique Is Your Web Browser?' in Mikhail J Atallah and Nicholas J Hopper (eds), *Privacy Enhancing Technologies*, vol 6205 (Springer Berlin Heidelberg, 2010) <<https://coveryourtracks.eff.org/static/browser-uniqueness.pdf>> accessed 12 May 2022.

Also, Nikiforakis N and Acar G, 'Browser Fingerprinting and the Online-Tracking Arms Race - IEEE Spectrum' (*IEEE Spectrum*, 25 July 2014) <<https://spectrum.ieee.org/browser-fingerprinting-and-the-onlinetracking-arms-race>> accessed 12 April 2022. To explore the how this works on your own browser, see <<https://coveryourtracks.eff.org/>> and the accompanying explanation.

¹²⁴ Disconnect, *Disconnect Tracking Protection - Tracker Descriptions* (2022) <<https://github.com/disconnectme/disconnect-tracking-protection/blob/5b190347aaeb088e0bb78388c6755243eaf4ff97/descriptions.md>> accessed 14 July 2022.

¹²⁵ Burgess M, 'The Quiet Way Advertisers Are Tracking Your Browsing' (*Wired*, 26 February 2022) <<https://www.wired.com/story/browser-fingerprinting-tracking-explained/>> accessed 14 July 2022.

on 25% of the top 10,000 Alexa-ranked sites worldwide¹²⁶, up from 0.4% in 2013¹²⁷.

Fingerprinting is often regarded as particularly invasive and difficult for users to circumvent. Reports suggest that even where cookies are deleted from a user's browser, the set of attributes used to fingerprint their device remain, allowing tracking to continue¹²⁸. Fingerprinting techniques are constantly evolving to draw on new attributes¹²⁹, especially considering that the number of characteristics that can be used to differentiate a specific user is essentially "open-ended"¹³⁰. Measures to prevent fingerprinting typically involve "masking" or "spoofing" these unique attributes to reduce the available "fingerprinting surface"¹³¹, although research from W3C found that "advances in techniques for browser fingerprinting [...] suggest that complete elimination of the capability of browser fingerprinting by a determined adversary through solely technical means that are widely deployed is implausible"¹³².

Google places limits on intermediaries' ability to use fingerprinting, though some in the ad industry have questioned the robustness of those limits¹³³. A recent study has found evidence of iOS apps "computing and agreeing on a fingerprinting-derived identifier through the use of server-side code", in breach of Apple's policies¹³⁴. Large scale surveys of tracking have identified the use of fingerprinting scripts on a minority of websites, with their purpose sometimes being unclear. In addition to its use for targeting and cross-device identification,

¹²⁶ Iqbal U, Englehardt S and Shafiq Z, 'Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors' (*arXiv*, 10 August 2020) <<http://arxiv.org/abs/2008.04480>> accessed 14 July 2022.

¹²⁷ Nikiforakis N and others, 'Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting', *2013 IEEE Symposium on Security and Privacy (IEEE, 2013)* <<http://ieeexplore.ieee.org/document/6547132/>> accessed 14 July 2022.

¹²⁸ Burgess M, 'The Quiet Way Advertisers Are Tracking Your Browsing' (*Wired*, 26 February 2022) <<https://www.wired.com/story/browser-fingerprinting-tracking-explained/>> accessed 14 July 2022.

¹²⁹ Iqbal U, Englehardt S and Shafiq Z, 'Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors' (*arXiv*, 10 August 2020) <<http://arxiv.org/abs/2008.04480>> accessed 14 July 2022.

¹³⁰ Datta A, Lu J and Tschantz MC, 'Evaluating Anti-Fingerprinting Privacy Enhancing Technologies', *The World Wide Web Conference (ACM, 2019)* <<https://dl.acm.org/doi/10.1145/3308558.3313703>> accessed 14 July 2022.

¹³¹ Datta A, Lu J and Tschantz MC, 'Evaluating Anti-Fingerprinting Privacy Enhancing Technologies', *The World Wide Web Conference (ACM, 2019)* <<https://dl.acm.org/doi/10.1145/3308558.3313703>> accessed 14 July 2022.

¹³² 'Mitigating Browser Fingerprinting in Web Specifications' (*W3.org*, 28 March 2019) <<https://www.w3.org/TR/fingerprinting-guidance/#research>> accessed 14 July 2022.

¹³³ Kaye K, 'Google's Opaque Practices to Restrict Fingerprinting Create Confusion among Its Ad Tech Partners' (*Digiday*, 3 June 2021) <<https://digiday.com/media/googles-opaque-practices-to-restrict-fingerprinting-create-confusion-among-its-ad-tech-partners/>> accessed 8 May 2022.

¹³⁴ Kollnig K and others, 'Goodbye Tracking? Impact of IOS App Tracking Transparency and Privacy Labels' (*arXiv*, 2022) <<http://arxiv.org/abs/2204.03556>> accessed 12 May 2022.

fingerprinting is also used for anti-fraud purposes by companies like DoubleVerify¹³⁵.

1.3.1.1.4 User Accounts

User accounts are used to identify individuals and can be strengthened through verification via a separate device (e.g. a mobile phone) and/or the addition of payment information. Verified user accounts unite an internal site or platform ID with a common identifier like an email address or telephone number, allowing data to be connected to an individual and used for advertising purposes.

Once a user is logged in to a platform, the platform can collect significant amounts of data about their behaviour. This can be data that signals interests, intent and location depending on the platform. Demographic data can also be collected as part of the account creation process.

Most Meta services require an account login even for passive browsing¹³⁶. Google products like Android, YouTube and Chrome can be used without logging in, but users are incentivised to log in to access additional functionality¹³⁷. Google and Facebook accounts can also be used to log in to a range of third-party services and websites, enabling them to collect additional data about users' behaviour. In its privacy policy, Facebook acknowledges that it collects information from "partners, vendors and third parties" who use "Meta Business Tools", including Facebook Login, to match "off-Facebook activity" to a user's account. This suggests that activities such as logging into a third-party service through Facebook can then be combined with a user's Facebook profile to target ads¹³⁸.

Some publishers require users to log in to access content (for free or as part of a subscription), but not all. Advertisers can use a number of incentives to encourage users to create verified user accounts on their sites and apps. Examples include

¹³⁵ See Englehardt S and Narayanan A, 'Online Tracking: A 1-Million-Site Measurement and Analysis', *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (ACM, 2016) <<https://dl.acm.org/doi/10.1145/2976749.2978313>> accessed 7 May 2022.

¹³⁶ Lazzari Z, 'How to Look at Facebook Without a Sign-On' (*Techwalla*, 28 September 2020s) <<https://www.techwalla.com/articles/how-to-look-at-facebook-without-a-sign-on>> accessed 12 May 2022; Okumoko J, 'How to View Instagram Posts Without an Account' (*Make Use Of*, 3 February 2022) <<https://www.makeuseof.com/how-to-view-instagram-without-account/>> accessed 12 May 2022.

¹³⁷ For example, YouTube requires age verification to access flagged videos on the platform. Possession of a standard Google account is accepted as proof of eligibility. Without a Google account, Android phone users need to use alternative app stores instead of Google Play.

¹³⁸ Nield D, 'All the Ways Facebook Tracks You—and How to Limit It' (*Wired*, 12 January 2020) <<https://www.wired.com/story/ways-facebook-tracks-you-limit-it/>> accessed 18 July 2022.

getting people to sign up for rewards or a loyalty programme, offering free gifts¹³⁹ or even direct cash payments¹⁴⁰.

To increase the scale of the data that can be collected and combined under a single user account, several initiatives have been launched by publishers, broadcasters, intermediaries, advertisers and other stakeholders, such as netID in Europe¹⁴¹. These initiatives aim to enable users to log in to a range of different websites and services using a single account, often linked to an email address. This means that data from multiple sources can be connected to each account and used for advertising purposes.

Email addresses and phone numbers can also be used as a “join key” to create new identifiers on a per site basis (i.e. without logging in to a user account), for example through LiveRamp’s Authenticated Traffic Solution (ATS). ATS allows publishers and advertisers to link data about an individual using an email address¹⁴². Data clean rooms such as InfoSum enable advertisers and publishers to upload data to a platform and match it using common identifiers (e.g. email address)¹⁴³.

Many advertising services run systems that take a list of identified people and certain other criteria (such as geographic scope), and then returns a targeting audience of users who are similar (by some proprietary definition of similarity) to the original list¹⁴⁴. Names, email addresses and telephone numbers can be uploaded as identifying keys. Facebook’s Custom Audience tool, for example, allows marketers to create target audiences based on uploading identifying keys such as names, email addresses or telephone numbers¹⁴⁵.

¹³⁹ For example, Budweiser’s 2021 Super Bowl campaign offered a free beer to anyone who shared their details with the company during a limited time period. Hein K, ‘Free Beer for Data: Brands up the Ante for First-Party Data Collection’ (*The Drum*, 3 March 2021) <<https://www.thedrum.com/news/2021/03/03/free-beer-data-brands-up-the-ante-first-party-data-collection>> accessed 8 May 2022.

¹⁴⁰ ‘Chipotle Rewards Launches By Giving Fans A Quarter Of A Million Dollars On Venmo’ (*Chipotle*, 12 March 2019) <<https://newsroom.chipotle.com/2019-03-12-Chipotle-Rewards-Launches-By-Giving-Fans-A-Quarter-Of-A-Million-Dollars-On-Venmo>> accessed 8 May 2022.

¹⁴¹ ‘European netID Foundation’ (*European netID Foundation*) <<https://enid.foundation/en/>> accessed 21 May 2022.

¹⁴² It is assumed that the advertiser has consent from the user to use their email address for this purpose.

¹⁴³ ‘Data Collaboration Platform’ (*Infosum*) <<https://www.infosum.com/platform>> accessed 5 May 2022.

¹⁴⁴ Facebook and Twitter run “lookalike audiences”; Google run “similar audiences”; Pinterest runs “actalike audiences”.

¹⁴⁵ ‘About Custom Audiences’ (*Facebook Business Help Centre*) <<https://en-gb.facebook.com/business/help/744354708981227>> accessed 7 May 2022.

1.3.1.2 The future of identity in advertising

Today, verified user accounts provide a basis for sites and services with a large number of users to collect first-party data for advertising purposes (e.g. on Google and Facebook). However, sites and apps with a smaller user base (e.g. local news publishers) tend to rely on cookie IDs and mobile IDs to identify users because they can be used to combine data from multiple sources. In addition, cookie and mobile IDs do not require users to log in, thereby reducing barriers to accessing content.

However, cookie IDs and mobile IDs are facing a decline. Google has announced that third-party cookies will become “obsolete” in Google’s Chrome browser¹⁴⁶, effectively cutting off the main source of data for cookie IDs in the future (Google Chrome represents 60% of browsers in the EU)¹⁴⁷. The two main mobile ID systems are also facing a decline. Apple’s ATT changes (see section 1.3.1.1.2) have led to high opt-out rates¹⁴⁸, which means less data is available to feed into mobile IDs on Apple devices. Google has also announced that the mobile ID on its Android operating system will cease to exist in the future.

All of these developments mean that cookie IDs and mobile IDs based on data collected from multiple sources are likely to play a much less significant role in digital advertising in the future. As a result, many industry stakeholders are looking at alternative ways to identify and profile individuals in order to compensate for these restrictions. Some of these alternatives are outlined below.

1.3.1.2.1 Shared User IDs

Verified user IDs are already used by some of the biggest platforms to identify users (e.g. on Google, and Facebook). The wide reach and diversity of services that these companies provide enables them to collect significant amounts of data that they use to increase the perceived value of their advertising products (see section 1.3.2). However, publishers (especially small ones) and advertisers are unlikely to be able to collect the same range and volume of data if they can only track activity on their own sites and apps. To tackle this challenge, a number of cross-industry initiatives involving advertisers, publishers, intermediaries, agencies and others have emerged which aim to create shared user IDs that individuals can use to log in to a wide range of sites and apps outside of “walled garden” ecosystems like Google and Meta. These shared user IDs would enable

¹⁴⁶ Schuh J, ‘Building a More Private Web: A Path towards Making Third Party Cookies Obsolete’ (*Chromium Blog*, 14 January 2020) <<https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>> accessed 7 May 2022.

¹⁴⁷ Amraoui NE, ‘Navigating the Post Third-Party Cookie Era’ (*AdTonos*, 18 March 2022) <<https://www.adtonos.com/navigating-the-post-third-party-cookie-era/>> accessed 8 May 2022.

¹⁴⁸ See section 1.3.1.1.2.

data about individuals to be collected across all participating sites and apps, and linked to a central identifier that can be used for advertising purposes. Many of these initiatives propose using email addresses as a join key¹⁴⁹, although some are exploring the use of first-party cookies¹⁵⁰ and probabilistic techniques to integrate additional data¹⁵¹.

Google has stated that it will not support many of these initiatives in Chrome in the future, arguing that they “don’t believe these solutions will meet rising consumer expectations for privacy, nor will they stand up to rapidly evolving regulatory restrictions”¹⁵². Instead, the company is encouraging the digital advertising industry to engage in a Google-led initiative to build alternative targeting methods called Privacy Sandbox.

1.3.1.2.2 Google’s Privacy Sandbox

In 2019, Google announced an initiative to “develop a set of open standards to fundamentally enhance privacy on the web”, called Privacy Sandbox¹⁵³. The next year, Google announced plans to “phase out” third-party cookies in Chrome¹⁵⁴, citing user demand and privacy concerns. Although many in the advertising industry raised concerns that this could have a negative impact on the way that ads are targeted and measured, Google provided reassurances that its Privacy Sandbox initiative would “sustain a healthy, ad-supported web in a way that will render third-party cookies obsolete”¹⁵⁵. In 2022, Google extended the scope of the Privacy Sandbox to its mobile operating system, Android¹⁵⁶.

Over the past three years, several proposals have been reviewed and discussed in the context of Google’s Privacy Sandbox. At the time of writing, eight proposals are under discussion or being tested under categories such as “show relevant

¹⁴⁹ For example, Unified ID 2.0 which uses ‘hashed and encrypted’ email addresses. Unified ID Solution 2.0 (*The Trade Desk*) <<https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0>>.

¹⁵⁰ ‘SWAN – Giving People Choice’ (SWAN) <<https://swan.community/>> accessed 5 June 2022.

¹⁵¹ ‘Future-Proofed User Identification for Digital Advertising’ (ID5) <<https://id5.io/>> accessed 7 May 2022.

¹⁵² ‘Charting a course towards a more privacy-first web’, (*Google Blog*) <<https://blog.google/products/ads-commerce/a-more-privacy-first-web/>> accessed 23 May 2022.

¹⁵³ Schuh J, ‘Building a More Private Web’ (*Google Blog*, 22 August 2019) <<https://www.blog.google/products/chrome/building-a-more-private-web/>> accessed 7 May 2022.

¹⁵⁴ Schuh J, ‘Building a More Private Web: A Path towards Making Third Party Cookies Obsolete’ (*Chromium Blog*, 14 January 2020) <<https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>> accessed 7 May 2022.

¹⁵⁵ Schuh J, ‘Building a More Private Web: A Path towards Making Third Party Cookies Obsolete’ (*Chromium Blog*, 14 January 2020) <<https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>> accessed 7 May 2022.

¹⁵⁶ Chavez A, ‘Introducing the Privacy Sandbox on Android’ (*Google Blog*, 16 February 2022) <<https://blog.google/products/android/introducing-privacy-sandbox-android/>> accessed 12 May 2022.

content and ads”, “measure digital ads” and “fight spam and fraud on the web”¹⁵⁷. This forum is open to all stakeholders and includes large platforms, publishers, intermediaries and agencies, although several participants have noted only limited participation from advertisers.

Google’s Privacy Sandbox and its main proposals are discussed in more detail in section 5.2.

1.3.2 Types of data collected

This section provides an overview of the different types of data collected for digital advertising purposes, grouped into five categories: demographic¹⁵⁸, interest¹⁵⁹, intent¹⁶⁰, location¹⁶¹ and measurement¹⁶². In reality, most of these categories overlap and intersect in many different ways, especially when linked to identifiers¹⁶³ that enable further inferences to be made based on cross-referencing and further profiling individuals. It is important to note that this constant and real-

¹⁵⁷ ‘How We’re Protecting Your Online Privacy’ (*Privacy Sandbox*)

<https://privacysandbox.com/intl/en_us/open-web/> accessed 12 May 2022.

¹⁵⁸ Demographic data is a category of personal data related to the “factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity” within the GDPR’s definition of personal data (Article 4.1 GDPR). *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

¹⁵⁹ Interest data is mentioned in the GDPR’s definition of profiling. Article 4.4 GDPR notes that profiling means “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.” *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

¹⁶⁰ Intent data is a data about users’ behaviour, which is mentioned in the GDPR’s definition of profiling. See footnote 159.

¹⁶¹ According to Article 2(c) ePrivacy Directive, location data means “any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.” 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), OJ L 201, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>.

¹⁶² Although EU law does not include a definition of measurement data, the proposal for an ePrivacy Regulation includes a description of what is typically defined as “frequency data”(see section 1.3.2.5.4), a subset of measurement data: data that is “necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.” Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD), <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>>.

¹⁶³ See section 1.3.1.1.

time “enrichment” of data in the digital advertising ecosystem can mean that the nature of the data can evolve. Some seemingly banal data points can be combined with others to generate detailed insights or inferences about an individual that individual data points or smaller data samples cannot do alone. In this context, sensitive categories of data may be revealed by such enrichment techniques.

Article 9.1 GDPR prohibits the processing of certain data, unless limited exemptions detailed in Article 9.2 GDPR apply. The GDPR categorises such data as “special category data”, which is data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and [...] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”.

The protections afforded by Article 9 are particularly acute in the digital advertising system, as the real-time enrichment of data may result in personal characteristics being “revealed” that are protected by Article 9. As advertising identifiers enable the ad ecosystem to build up detailed profiles of individuals using data from different sources, those profiles can involve the processing of special categories of data, even if the original data collected would not fall under Article 9 GDPR. This means that processing of the types of data outlined below could involve special category data in some way.

1.3.2.1 Demographic data

Demographic data usually includes information about a person’s gender, age, education level and income. However, standard industry definitions of demographic data can also include purchasing history and personal preferences¹⁶⁴.

Google, Facebook, and other platforms request some demographic attributes during account registration. It is increasingly common for sites to gate access to free content and commenting systems with a registration requirement, which can involve requesting demographic attributes or an email address that can be used to cross-reference against data broker records or other sources. This data can also be collected or inferred when a payment is made (e.g. for subscriptions, or to purchase access to a service).

Demographic data can also be inferred from an individual’s browsing patterns and search history. In 2013, a group of Microsoft researchers developed a method for

¹⁶⁴ ‘Glossary of Terminology’ (IAB) <<https://www.iab.com/insights/glossary-of-terminology/>> accessed 7 May 2022.

inferring the age and gender of search users with 77-84% accuracy¹⁶⁵. More recently, in 2018, Kostakos et al. developed a method to infer the age of Twitter users from their profile pictures¹⁶⁶. The DMP 1plusX, which counts publisher Axel Springer among the clients listed on its website, scores articles and pages using machine learning and predictive analytics to guess the gender and age of the reader¹⁶⁷.

Demographic data relies on being tied to an identifier in order to be useful, because individuals usually only explicitly provide this information infrequently (for example, when creating a new user account on a platform). When demographic data is inferred, it needs to be linked to other data sources through a common identifier.

In 2019, Neuman et al., citing surveys by Salesforce and Lotame, indicated that demographic information remains the most popular form of data with advertisers¹⁶⁸. However, two advertisers interviewed for this study indicated that demographic data is decreasing in importance¹⁶⁹. This may be linked to concerns around the accuracy of demographic data that is currently made available in the digital advertising ecosystem by third parties: one study found that gender data sourced from data brokers is accurate less than 50% of the time, or “less efficient than using nothing”¹⁷⁰. Similarly, data from audience measurement, data and analytics company Nielsen suggests that, on average, ads based on profiling only reach their intended demographic 63% of the time¹⁷¹. However, studies have shown that demographic data collected or inferred by Facebook and Google tends to be more accurate¹⁷².

¹⁶⁵ Bi B and others, ‘Inferring the Demographics of Search Users: Social Data Meets Search Queries’, *Proceedings of the 22nd international conference on World Wide Web - WWW ‘13* (ACM Press, 2013) <<http://dl.acm.org/citation.cfm?doi=2488388.2488401>> accessed 7 June 2022.

¹⁶⁶ P. Kostakos and others, ‘Inferring Demographic Data of Marginalized Users in Twitter with Computer Vision APIs’, *2018 European Intelligence and Security Informatics Conference (EISIC, 2018)* <<https://ieeexplore.ieee.org/document/8752947>>.

¹⁶⁷ 1plusx | AI-Powered Data Management Platform’ (*1plusX*) <<https://www.1plusx.com/>> accessed 7 June 2022.

¹⁶⁸ Neumann N, Tucker CE and Whitfield T, ‘How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies’ [2019] *Marketing Science*, 38(6):918-926, <<https://pubsonline.informs.org/doi/10.1287/mksc.2019.1188>> accessed 5 June 2022.

¹⁶⁹ Advertiser 1, Advertiser 6 – see part B for more detail on interviews carried out for this study.

¹⁷⁰ Neumann N, Tucker CE and Whitfield T, ‘How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies’ [2019] *Marketing Science*, 38(6):918-926, <<https://pubsonline.informs.org/doi/10.1287/mksc.2019.1188>> accessed 5 May 2022.

¹⁷¹ ‘Advertiser Playbook: Strategies and Tactics for 2022 Planning’ (Nielsen, 21 October 2021) <<https://www.nielsen.com/us/en/insights/report/2021/advertiser-playbook/>>.

¹⁷² Grow A and others, ‘How Reliable Is Facebook’s Advertising Data for Use in Social Science Research? Insights from a Cross-National Online Survey’ (Max Planck Institute for Demographic Research 2021) WP-2021-006 <https://www.demogr.mpg.de/en/publications_databases_6118/publications_1904/mpidr_working_papers/how_reliable_is_facebook_s_advertising_data_for_use_in_social_science_research_insights_from_a_cross_national_online_survey_6991> accessed 7 April 2022; Tschantz MC and others, ‘The Accuracy of the Demographic Inferences Shown on Google’s Ad Settings’ (*arXiv*, 2018) <<http://arxiv.org/abs/1808.07549>> accessed 7 May 2022.

1.3.2.2 Interest data

Companies can gain knowledge of user interests based on observation of site or app interaction and usage. Examples may include content considered to be engaging for a user (e.g. read, liked, commented, shared), the groups a user is a member of (e.g. "second-hand luxury cars for sale in Luxembourg"), ads they interact with (e.g. viewed, clicked). These data points are recorded by analytics systems, or used to profile users and generate "segments" that can be used to target advertising.

This type of data is strongly dependent on the type of site or app being used. News publishers can observe people's interaction with articles and other types of content on their sites and apps, while platforms like Google can observe what people are searching for (Google Search), what activities and services people are looking for in different locations (Google Maps), what websites people visit (Google Chrome), what apps they download and how they use them (Android) and people's interaction with video content (YouTube). All of this data can be used to build up a picture of a person's interests and intentions, which can be used to target ads.

Where third-party identifiers are available, data brokers can allocate additional interests derived from a broader range of browser history and offline data. For example, Quantcast, an analytics and advertising company, compiles data from many sources to produce targeting insights¹⁷³. Because Quantcast's tags are present on many publishers' websites, the company has access to large parts of a user's browsing history. In addition to "raw" data, Quantcast can also integrate segment data acquired from data brokers such as Oracle Data Cloud, Experian and Acxiom¹⁷⁴.

Most interest data is inferred. Identifiers are used to link individuals to different interest categories over time. For example, Permutive, a DMP, offers a "first impression" service where pages browsed by a new visitor are analysed and this information puts the user into a "segment" that can be used for targeting ads. As further data about the user accumulates, this segment selection is refined¹⁷⁵.

Interest data can also be collected based purely on the context of the content where the ad is going to be displayed. For example, publishers can generate their

¹⁷³ 'Explore the Future of Cookieless Advertising' (*Quantcast*) <<https://www.quantcast.com/>> accessed 7 May 2022.

¹⁷⁴ Kaltheuner F, 'I Asked an Online Tracking Company for All of My Data and Here's What I Found' (*Privacy International*, 7 November 2018) <<http://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>> accessed 7 May 2022

'Control the Ads You See' (*Google Account Help*) <<https://support.google.com/accounts/answer/2662856>> accessed 7 May 2022.

¹⁷⁵ 'Audience Platform for Publishers' (*Permutive*) <<https://permutive.com/audience-platform/publishers/>> accessed 7 May 2022.

own category descriptions for their content or use the standardised taxonomy published by the IAB Tech Lab, which is widely used by buyers and sellers¹⁷⁶. Multiple categories can be used for a piece of content, and may be applied at the page, section and site level. Machine learning is widely applied to content to try and better understand how interest data can be used for targeting. Technology vendors use natural language processing (NLP) and computer vision to grasp the textual meaning and classify any images present on the page, which is also relevant for ad verification. Images can be further classified based on whether they contain people, products, objects or locations, for example. Voice to text tools are used to create transcripts out of audio/video content, which allows for closer analysis and classification. Some companies offer “sentiment” analysis to judge whether the tone is positive or negative and predict the emotional effect on the reader. This type of data is often linked to identifiers and supplemented with other connected data including demographics, additional interests and intent in order to increase the value of the ad inventory. In turn, the GDPR would apply to such data, given the broad definition of personal data provided for in the GDPR.¹⁷⁷

1.3.2.3 Intent data

While interest data is a useful marker for relevance, it does not mean that the user is “in the market” for related goods or services at any given time. Intent data, by contrast, can show that the user is actively considering a purchase.

Search is the best general source of intent data because this is where consumers commonly begin to research a potential purchase. Google (whose share of the global search engine market was approximately 92% in 2022)¹⁷⁸ can use this data to inform the selection of ads shown in its search advertising products as well as on its display networks. Specialist search services can have access to a narrower spectrum of intention signals in fields such as travel and automotive.

Amazon and other e-commerce platforms have access to search and purchase data from their sites and apps. At a smaller scale, some e-commerce retailers will have data on, for example, items left in shopping baskets and product pages viewed. This has enabled “merchant media” to become a growing digital advertising channel. A recent BCG report (in partnership with Google) estimates that merchant media will grow by 25% per year over the next five years in the

¹⁷⁶ IAB Tech Lab, Content Taxonomy, (*IAB Tech Lab*) <<https://iabtechlab.com/standards/content-taxonomy/>> accessed 22 May 2022.

¹⁷⁷ *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

¹⁷⁸ ‘Search Engine Market Share: Who’s Leading the Race In 2022’ (*Kinsta*, 2022) <<https://kinsta.com/search-engine-market-share/>> accessed 6 October 2022.

US¹⁷⁹, and Ebiquty analysis has estimated that Amazon's advertising revenue increased by 63% between 2020 and 2021¹⁸⁰.

Google claims that intent data is significantly more effective than demographic data – so much so that “marketers who rely only on demographics to reach consumers risk missing more than 70% of mobile shoppers”¹⁸¹.

Search queries are usually associated with account IDs where available, and with unique cookies otherwise. Similarly, retailers that collect intent data through their sites and apps can link this information to a user account or, if a user is not logged in, to a unique cookie. Without an identifier, the delivery of ads based on intent data would be limited to the environment in which the intent data was originally collected (e.g. within a list of search results, or on a retailer site). This means that intent data becomes significantly more valuable when linked to an identifier, as it enables advertisers to target individuals throughout their “path to purchase” rather than just at one specific moment.

1.3.2.4 Location data

User location is a key relevance vector for digital advertising. It reveals where people go and how long they stay there, which aids inferences regarding home, workplace and family status, among others¹⁸². Location can also be used to trigger local ads when a device enters a defined geofenced area, which is only possible if the device's position is regularly updated. This mostly concerns mobile devices, but could also apply to other types of portable device such as laptops and connected devices such as smart watches.

Precise location can be gathered using GPS data. Further granularity is available if wi-fi is turned on or wi-fi scanning enabled. Google does not publish figures on the number of users who opt in to location services, but in correspondence with the CMA they stated that in the UK it is in the range of “half to two-thirds” of Android users¹⁸³. However, users do not always explicitly provide this information

¹⁷⁹ Wiener L and others, 'How Retail Media Is Reshaping Retail' (*BCG Global*, 23 March 2022) <<https://www.bcg.com/publications/2022/how-media-is-shaping-retail>> accessed 7 May 2022.

¹⁸⁰ 'Ebiquty Plc on LinkedIn: Now That Amazon Has Posted Their Q4 Earnings for 2021, Following Alphabet' (*LinkedIn*) <https://www.linkedin.com/posts/ebiquity-plc_now-that-amazon-has-posted-their-q4-earnings-activity-6895115061984378880-p_sj> accessed 7 May 2022.

¹⁸¹ Gevelber L, 'Why Consumer Intent Is More Powerful than Demographics' (*Think With Google*, December 2015) <<https://www.thinkwithgoogle.com/consumer-insights/consumer-trends/why-consumer-intent-more-powerful-than-demographics/>> accessed 7 May 2022.

¹⁸² For example, Google's privacy policy explains that “Google uses location information in our ads products to infer demographic information, to improve the relevance of the ads you see, to measure ad performance and to report aggregate statistics to advertisers.” 'Privacy & Terms' (*Google*) <<https://policies.google.com/technologies/ads?hl=en>> accessed 28 May 2022.

¹⁸³ See 'Appendix G: the role of tracking in digital advertising', in 'Online Platforms and Digital Advertising - Market Study Final Report' (*Competition and Markets Authority*, 2020), p. G103

for advertising purposes; usually the purpose is combined with other functionalities (e.g. for maps).

To access the GPS data of a mobile device, an app must obtain the user's permission. This permission may be necessary for the functionality of the app or required as a result of the addition of third-party code (SDKs). While the most prevalent SDKs belong to Google and Meta¹⁸⁴, other actors also offer location SDKs, such as Groundtruth, Cubiq, mParticle, and PlaceID. Many apps collecting the data sell it on the open market or package it for data brokers and process it as part of other products.

Where GPS data is unavailable, as is the case on laptop and desktop machines without GPS cards (e.g. Apple MacBooks), location can be derived from wi-fi scanning and connections to a high level of accuracy¹⁸⁵. Databases of public wi-fi hotspots can be matched to geolocation coordinates. The method of last resort, however, is to do a GeoIP look up on the user's IP address. Depending on the connection, this may give a relatively precise result (university or workplace with a permanent IP range) or one that is coarser, such as a city neighbourhood.

Recent reports suggest that accelerometer data is being captured systematically from iPhones¹⁸⁶. Accelerometer data – which is not protected by device permissions and includes gyroscope and barometer readings – allows the recipient to identify the device's altitude and orientation. This could enable companies to look for other users at the same altitude whose location settings are enabled, and make a good inference about the location of the original phone as a result.

The language used in a media context is also a strong pointer to the location of the potential audience, and references to places in the media may suggest that products or services connected to or serving that locality are relevant. When combined with the timestamp of the impression, it could be possible to guess at the time of day, which may contextualise the user's activity (work, leisure) and the likelihood of their making a purchase.

<https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf>.

¹⁸⁴ 'Appendix G: the role of tracking in digital advertising', in 'Online Platforms and Digital Advertising - Market Study Final Report' (*Competition and Markets Authority*, 2020), <https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf>.

¹⁸⁵ 'Wi-Fi Positioning System' (*Wikipedia*) <https://en.wikipedia.org/wiki/Wi-Fi_positioning_system#Public_Wi-Fi_location_databases> accessed 12 May 2022.

¹⁸⁶ Ikeda S, 'Facebook's Use of Alternate Location Tracking Methods To Circumvent Apple Privacy Protections Expands to Accelerometer Data' (*CPO Magazine*, 5 November 2021)

<<https://www.cpomagazine.com/data-privacy/facebooks-use-of-alternate-location-tracking-methods-to-circumvent-apple-privacy-protections-expands-to-accelerometer-data/>> accessed 12 June 2022.

Location data is valuable for ad targeting because it enables advertisers to restrict advertising only to individuals in locations where an advertising campaign is relevant. For example, a bar owner interviewed for this study was only interested in showing ads to people in the area where his bar is located¹⁸⁷. Location can also be used to infer other types of data that could be used to target ads. For example, through IBM Watson Advertising, IBM allows advertisers to use location data to target ads using weather¹⁸⁸ or COVID-19 indicators¹⁸⁹. Global advertiser Unilever, for example, has used location and weather indicators to target ice cream ads to individuals using “thermal targeted proximity messaging”¹⁹⁰. There is significant perceived value associated with being able to track people’s locations over time, especially for measurement, but such location data is likely to involve personal data to which the GDPR applies.

1.3.2.5 Measurement data

Measurement refers to the evaluation of the performance of digital ads. The basis of measurement is data describing whether or not an ad was viewed, how many people saw it, how many times an ad was shown to a particular person, and what actions were taken by the people that saw the ad. It is typically a high priority for advertisers¹⁹¹, because it enables them to optimise their budget on the basis of their objectives (e.g. brand awareness, sales, customer retention). The most important categories of measurement data for advertisers include¹⁹²:

- **Impressions:** the number of times an ad was served.
- **Viewability:** whether an ad was actually seen by users.
- **Reach:** the number of unique users which saw an ad.
- **Frequency:** how many times users were exposed to the same ad.
- **Engagement:** how many people engaged in some way with an ad they were shown, such as clicking on it, swiping the content, expanding an image.

¹⁸⁷ Advertiser 6 – see part B for more detail on interviews carried out for this study.

¹⁸⁸ ‘The Complete Guide for Weather-Triggered Advertising’ (*IBM Watson Advertising*, 9 July 2021) <<https://www.ibm.com/watson-advertising/thought-leadership/complete-guide-weather-triggered-advertising>> accessed 18 May 2022.

¹⁸⁹ ‘IBM Watson Advertising COVID-19 Triggers’ (*IBM Watson Advertising*, 11 September 2020) <<https://www.ibm.com/watson-advertising/thought-leadership/covid-19-triggers>> accessed 18 May 2022.

¹⁹⁰ Kaffash J, ‘Wall’s and O2 Target Ads around Weather’ (*Marketing Week*, 9 August 2012) <<https://www.marketingweek.com/walls-and-o2-target-ads-around-weather/>> accessed 2 June 2022.

¹⁹¹ Kirkpatrick D, ‘Study: Most Marketers List Advanced Attribution as a Top Priority’ (*Marketing Dive*, 17 May 2016) <<https://www.marketingdive.com/news/study-most-marketers-list-advanced-attribution-as-a-top-priority/419319/>> accessed 12 May 2022.

¹⁹² ‘WFA Global Position on Advertiser Access to Data in the Digital Advertising Market’ (*World Federation of Advertisers*, 9 April 2021) <<https://wfanet.org/knowledge/item/2021/04/09/WFA-global-position-on-advertiser-access-to-data-in-the-digital-advertising-market>> accessed 7 June 2022.

- **Conversion:** to what extent an ad led to people taking a particular action (e.g. buying a product, filling out a contact form).

Depending on advertisers' goals, the importance of different categories of measurement data will vary. For example, impressions, viewability, reach and frequency data are important for assessing whether a campaign was successful in increasing brand awareness. Meanwhile, engagement and conversion data are important for campaigns with objectives related to driving sales. The use of ad verification services, which ensure that ads are viewable, fraud-free and brand safe, can also be essential to measuring the performance of ads¹⁹³.

Advertisers have expressed a number of concerns regarding the validity of measurement data on large platforms. For example, during the preparation of its market study on online platforms and digital advertising, the CMA received feedback from advertisers expressing frustration at limited access to measurement data on Google and Facebook¹⁹⁴. In 2019, Meta settled a lawsuit and admitted to inflating its video-viewing metrics over an 18-month period¹⁹⁵. Section 4.3.1 provides more detail on advertisers' concerns related to measurement data, based on interviews.

1.3.2.5.1 Impressions

Measuring impressions involves counting the number of times an ad was served. Impressions are the basis for individual ad transactions. Advertisers and publishers typically rely on a CPM model to quantify the amount paid per thousand impressions.

There are two ways of measuring impressions¹⁹⁶:

- **Server-initiated:** impressions can be counted by the ad server each time an ad is transmitted to a publisher. This has limitations in that it involves counting impressions based on how many times an ad was delivered, rather than each time it was viewed by a user.

¹⁹³ See section 1.2.2.4.7.

¹⁹⁴ See 'Appendix O: measurement issues in digital advertising' in 'Online Platforms and Digital Advertising - Market Study Final Report' (*Competition and Markets Authority*, 2020), p. O13, <https://assets.publishing.service.gov.uk/media/5fe495ede90e071205803986/Appendix_O_-_measurement_issues_in_digital_advertising_WEB.pdf>.

¹⁹⁵ Spangler T, 'Facebook to Pay \$40 Million to Settle Claims It Inflated Video Viewing' (*Variety*, 7 October 2019) <<https://variety.com/2019/digital/news/facebook-settlement-video-advertising-lawsuit-40-million-1203361133/>> accessed 7 June 2022.

¹⁹⁶ 'Understanding Impressions in Digital Marketing To...'
(*BigCommerce*, 7 April 2022) <<https://www.bigcommerce.com/ecommerce-answers/impressions-digital-marketing/>> accessed 7 June 2022;

Schwarz C, 'What Are "Impressions"? A History of Impression Measurement in the Digital Advertising Industry' (*pixalate*, 9 October 2019) <<https://www.pixalate.com/blog/history-of-digital-ad-impression-measurement-infographic>> accessed 7 June 2022.

- **Client-initiated:** impressions can be counted by the browser or mobile app on which the user is seeing the ad (the “client”). This is typically more accurate, as browsers and apps are typically able to identify user behaviours that could prevent the ad from being viewed, such as the use of ad blocking software, the use of screen resolutions that are too low for the ad to appear and minimised browser windows.

1.3.2.5.2 Viewability

Measuring the performance of digital ads can be challenging, in part because the composition of the websites and apps that host ads can vary greatly. For example, every time a publisher launches a bid for an impression, its ad server specifies the size of the ad space available, its position on the page, and the type of device the ad is being viewed on. Measuring viewability therefore helps ensure that the impression was actually as described, and that a user actually saw the ad in question. What counts as a view, in terms of how much an ad was viewed and for how long, is defined via industry standards¹⁹⁷. For example, the IAB viewability standard for an average banner ad requires that 50% of the ad was viewed for a minimum of one second.

Viewability is typically measured through verification tags¹⁹⁸ loaded on the publisher page where the ad is displayed. This tag reports the URL and viewability data to a server controlled by the verification service, which is typically procured by the buy-side (advertisers, agencies, DSPs). On mobile apps, a similar process takes place through an SDK integrated into the app. This can happen on a cross-vendor basis, such as through IAB’s Open Measurement SDK¹⁹⁹.

1.3.2.5.3 Reach

Reach refers to the number of individual users that saw an ad. It is a key metric for campaigns focused on increasing brand awareness. The number of individual users that were reached by an ad is typically measured through the use of unique identifiers such as cookies.

1.3.2.5.4 Frequency

Whereas impressions measure how many times an ad has been served, and reach is a measure of how many individual users saw an ad, frequency is the number of impressions served per unique user (i.e. how many times an individual user has

¹⁹⁷ ‘Quick Q&A - Viewability’ (IAB UK, 3 April 2017) <<https://www.iabuk.com/news-article/quick-ga-viewability>> accessed 7 April 2022; ‘MRC Viewability Standards - A Quick Reference Guide’ (Automatad, 14 August 2019) <<https://headerbidding.co/mrc-viewability-standards/>> accessed 14 May 2022.

¹⁹⁸ See also 1.3.2.6.5.

¹⁹⁹ ‘Open Measurement SDK’ (IAB Tech Lab) <<https://iabtechlab.com/standards/open-measurement-sdk/>> accessed 22 May 2022.

been exposed to a single ad). Frequency capping is the practice of setting a limit on the number of times an ad should be shown to an individual user in order to reduce waste, overexposure and annoyance. Frequency is typically measured and capped through DSPs and buying systems used by advertisers. As with reach, identifiers such as cookies are typically used to count impressions delivered to individual users.

1.3.2.5.5 Engagement

Engagement refers to the extent to which a user engaged with an ad. The IAB describes three categories of engagement²⁰⁰:

- **Behavioural/physical:** refers to the physical actions individuals made when seeing the ad. This can include how long they looked at the ad and their interactions with it (e.g. clicks, hovers, swipes, video plays), as well as their social media interactions (e.g. likes, shares, follows). How long a user looked at an ad can be measured through browsing data or eye tracking (which involves biometric data), whereas interactions are measured through web and social analytics.
- **Cognitive:** when an individual changes the way they think after seeing an ad. This can include ad or campaign awareness, being able to recall the brand's message or attributes, or changing their purchase intent. This is usually measured through surveys.
- **Emotional:** when an individual changes the way they feel after seeing an ad, such as by changing the way they perceive or value a brand, by changing their loyalty to the brand in question, or by having a physiological response to the ad (e.g. changes in breathing, heart-rate). Other than the physiological response (which can be measured through biometric data), other forms of emotional engagement can only be measured through surveys.

1.3.2.5.6 Conversion

Measuring conversions involves identifying how many times an individual's view of an ad led to a particular action (e.g. purchase of a product, creation of an account or subscription to a service).

Conversions can be measured either as view-through (the user does not click the ad but still takes the desired action) or click-through (the user clicks the ad and

²⁰⁰ 'Defining and Measuring Digital Ad Engagement in a Cross-Platform World' (IAB, 2015) <https://www.iab.com/wp-content/uploads/2015/05/Ad_Engagement_Spectrum2014_FINAL2-5-2014-EB.pdf>.

takes the desired action). Click-through conversions are counted using click counters on publishers' ad servers. When users click, they are redirected to a service which counts that action before being delivered to the brand's landing page. Users can also be redirected to the advertiser's ad server before reaching the brand's landing page. This enables the advertiser to keep its own tally, which it can check against invalid traffic²⁰¹.

Tags can be placed on the page where ads are served and where the conversion event (e.g. a sale) takes place. The cookie ID set on the ad can then be matched with the conversion pixel when the desired action is taken, allowing the advertiser to know that a user who clicked on a certain ad took a certain action.

1.3.2.6 Other means of data collection

This section will provide an overview of other means of data collection within the digital advertising supply chain.

1.3.2.6.1 Embedded video players

Websites often use third-party services to host media files, such as videos and audio clips. This reduces their technical overheads and allows them to benefit from the quality of service associated with specialist providers. Where YouTube or another third-party host is used, that service will typically receive the IP address, referrer URL, user agent, and have the chance to set their own cookies on the browsers that visit the website²⁰². This is the case with all embedded media such as video, audio and posts from social media sites. For example, even if the user does not click on the embedded YouTube video, a cookie will be set and, if they are logged in to a Google account, this action can be associated with their account and could be used to influence which videos and ads they see in the future²⁰³. In cases where the user is unknown or not logged in to their Google account, a unique cookie can still be set that will remember that the user visited the website in question. Google offers a "privacy enhanced" mode for YouTube, which does not set personalisation cookies immediately on load, but only when the video is played. Nonetheless, the user's IP address and current URL are still transmitted, and YouTube also sets a unique identifier in local storage on the user's device²⁰⁴.

²⁰¹ 'Tracking and Reporting Impressions, Clicks, and Conversions in AdTech Platforms' *The AdTech Book* (Clearcode, 6 August 2019) <<https://adtechbook.clearcode.cc/tracking-reporting/>> accessed 16 May 2022.

²⁰² Tolvanen H, 'Are You Using Embedded YouTube Videos on Your Website? Read This!' (*LinkedIn*) <<https://www.linkedin.com/pulse/you-using-embedded-youtube-videos-your-website-read-heikki-tolvanen>> accessed 27 May 2022.

²⁰³ 'How Google Uses Information from Sites or Apps That Use Our Services' (*Google*) <<https://policies.google.com/technologies/partner-sites?hl=en>> accessed 7 May 2022.

²⁰⁴ This can be selected when generating an embed code and uses the <https://www.youtube-nocookie.com> domain, see 'Embed Videos and Playlists' (*YouTube Help*)

1.3.2.6.2 ReCAPTCHA

ReCAPTCHA is a Google-developed widget which tests whether a given visitor to a website is a human or a bot (e.g. by asking them to identify the content of specific pictures). Its latest iteration does not query the user, instead it captures and scores their behaviour on the site to assess whether they are human. This data is transmitted to Google²⁰⁵. According to analysis commissioned by the Australian Office of the Information Commissioner (OAIC), ReCAPTCHA requires that third-party cookies be enabled and that it set a cookie used by Google for advertising purposes²⁰⁶. Google responded that it uses data collected from the service only for security and not for advertising purposes^{207, 208}.

1.3.2.6.3 Social plugins

Social plugins such as Facebook's "Like" and "Share" buttons²⁰⁹ are commonly used by websites as tools for content promotion. According to company documents submitted to the US Congress in June 2018, Facebook's "Like" button appeared on 8.4 million websites and the "Share" button on 931,000 websites covering 275 million webpages²¹⁰. In 2021, Meta announced that this data about users would only be collected if they are logged in to Facebook and have given consent to Facebook's app and website cookies²¹¹. The European Court of Justice (CJEU) ruled

<<https://support.google.com/youtube/answer/171780?hl=en-GB#zippy=%2Cturn-on-privacy-enhanced-mode>> accessed 7 May 2022.

²⁰⁵ 'ReCAPTCHA v3 Usage Statistics' (*Built With*) <<https://trends.builtwith.com/widgets/reCAPTCHA-v3>> accessed 12 May 2022.

²⁰⁶ Johnston A and Culnane C, 'Cookies and Other Online Identifiers' (*Salinger Privacy*, 15 June 2020) <https://www.oaic.gov.au/_data/assets/pdf_file/0017/2465/20-06-15-research-paper-for-oaic-online-identifiers.pdf>.

²⁰⁷ Kan M, 'Cloudflare Dumps Google's ReCAPTCHA Over Privacy Concerns, Costs' (*PC Mag*, 9 April 2020) <<https://uk.pcmag.com/rss-tools/125583/cloudflare-dumps-googles-recaptcha-over-privacy-concerns-costs>> accessed 16 July 2022.

²⁰⁸ In a FAQ for developers, it is stated that the cookie necessary for the service is _GRECAPTCHA and that it is possible to set it on www.recaptcha.net instead of www.google.com if there are concerns about other cookies set on the former domain. See 'Frequently Asked Questions | ReCAPTCHA' (*Google Developers*) <<https://developers.google.com/recaptcha/docs/faq>> accessed 17 May 2022.

²⁰⁹ 'What Information Does Facebook Get When I Visit a Site with the Like Button?' (*Facebook Help Centre*) <https://www.facebook.com/help/186325668085084/?helpref=related_articles> accessed 24 May 2022; 'Business Tools Terms and Conditions' (*Facebook*) <<https://www.facebook.com/legal/terms/businessstools>> accessed 17 May 2022.

²¹⁰ Facebook's submission responding to questions for the record from US Energy and Commerce Committee hearing on "Facebook: Transparency and Use of Consumer Data", April 11, 2018 at p. 23 <<https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf>> accessed 18 June 2022.

²¹¹ 'Social Plugins' (*Facebook*) <<https://developers.facebook.com/docs/plugins/>> accessed 27 July 2022.

in 2019 that a website which embeds the “Like” button may be a joint controller in the collection and disclosure of the user data transmitted to Meta²¹².

1.3.2.6.4 Pixels

The Meta pixel provides analytics capacity to website owners. It is installed on 40-50% of sites in the UK²¹³. The website owner can select or define “events” on the page which will trigger the pixel to report data to Meta. Typical events could include placement of an item in a shopping cart or content viewed in a specific location on the page.

The pixel is a small piece of code that is usually added to the page template so that it is integrated throughout the site. As code, it has two parts: the first is a piece of JavaScript, which will usually be used to send the data. If JavaScript is not available then it uses a HTML call to load a tiny image (the pixel) and passes event data as an appended tag or URL parameter.

Meta additionally offers conversion and “custom audience” pixel tools which can track conversions and enable website owners to target users using Facebook ads. These services use a different URL to the Meta pixel²¹⁴.

1.3.2.6.5 Ad serving

Ad tags are pieces of code and other elements used to serve and measure advertising in web pages. For example, a publisher’s tag will describe the size and format of the creative required for an ad placement. Tags can be blocks of JavaScript code or HTML elements. The automated sale of ads can be operationalised by tags either inserted directly into the HTML or by a tag manager²¹⁵.

When a user visits a webpage, the browser can read the tag and send a request for an ad to the publisher’s ad server. This server stores details of the publisher’s direct deals with advertisers, and if the placement cannot be filled by an ad associated with a direct deal, the request is passed to an SSP. A call may also be

²¹² Case C-40/17 (Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV)

<<https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=162183>>.

²¹³ ‘Online Platforms and Digital Advertising - Market Study Final Report’ (Competition and Markets Authority, 2020), p. 16

<https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>.

²¹⁴ ‘Conversion Tracking | Meta Pixel Documentation’ (Facebook for Developers)

<<https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>> accessed 2 August 2022.

²¹⁵ See Zawadziński M, ‘What Is an Ad Server and How Does It Work?’ (Clearcode, 7 March 2018)

<<https://clearcode.cc/blog/what-is-an-ad-server/>> accessed 8 July 2022.

made to a DMP to “enrich” the data about the user, if available. This may include demographic attributes, audience segments and location data. The SSP then broadcasts a “bid request” to potential buyers who bid in an auction for the ad space²¹⁶. The winner’s tag will be loaded onto the web page and call the ad creative from the advertiser’s web server. The advertiser’s ad server or DSP may also drop measurement tags²¹⁷.

Publisher ad servers (e.g. Google’s Ad Manager) organise the filling of available inventory and measure click-through rates, while advertiser ad servers host creative and control the cadence and measurement of the ad campaign.

1.3.2.6.6 Fonts

Google hosts resources which are “hotlinked” by site owners both for the design and enhancements of website functions. This is driven by convenience: developers could store the fonts elsewhere, or the browser companies could ship their software with font packages included. When a user loads a site reliant on such components, a request is made by the browser to Google and can transfer data about the user’s browsing location. This transmission includes a referrer and other data²¹⁸. However, cookies are not used by Google to record font access, and the interaction is handled by dedicated resource specific domains.

In January 2022 a Bavarian court ordered a site to cease use of Google hosted fonts. The site claimed that the processing of user data invoked by the loading of fonts had a legal basis based on legitimate interest. The Court did not agree²¹⁹.

1.3.3 How data collection is communicated to users by Meta and Google

This section provides an overview of how Meta and Google communicate about their collection of data in their privacy policies and terms of service. This section focuses on these two companies because of the central role they play in the digital

²¹⁶ The bid request contains information about the user including identifiers, segment information, location data, page context etc. For more detail see Appendix 1-4 in Ryan J, ‘Behavioural Advertising and Personal Data’ (*Brave*, 2018) <<https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf>>.

²¹⁷ For more information on measurement, see section 1.3.2.5.

²¹⁸ “Our systems are designed to remove HTTP referrer information before logging, to avoid associating requests with any individual website using the Google Hosted Libraries.” ‘Google Hosted Libraries Terms of Service’ (*Google Developers*) <<https://developers.google.com/speed/libraries/terms>> accessed 15 July 2022.

²¹⁹ See Claburn T, ‘Google Fonts Lands Website Privacy Fine by German Court’ (*The Register*; 31 January 2022) <https://www.theregister.com/2022/01/31/website_fine_google_fonts_gdpr/> accessed 16 July 2022.

advertising ecosystem (see section 1.1.2), as well as their capacity to collect large amounts of individuals' data (see section 1.3).

1.3.3.1 Meta's data policy

Meta's policies confirm that it collects data that would fit into the above categories of demographic, intent, interest and location data as part of its users' use of its products (e.g. creation of profiles, activities on its platforms)²²⁰. Meta also states that it collects personal data provided by advertisers, app developers and publishers through the Meta Business tools that these partners use. These include social plug-ins (such as the "Like" button), Facebook Login, APIs, SDKs and the Meta pixel²²¹. Meta asserts that this allows them to collect data on users' activities when they are not using Meta platforms, including "information about [the user's] device, websites [users] visit, purchases [users] make, the ads [users] see and how [users] use their [partners'] services". The "privacy policy" includes links to Meta's APIs and SDKs with individual descriptions of each²²², and a link to a page targeted at business users describing the purpose and function of the Meta pixel²²³. It notes that the Meta pixel is used to measure cross-device conversions, optimise ad delivery, create custom audiences and to learn about website traffic.

Meta's data policy²²⁴ describes the legal bases it uses for various data processing purposes in detail. Meta relies primarily on their contract with their users as their lawful basis for processing, citing Article 6.1(b) GDPR. Meta's data policy states that "for all people who have legal capacity to enter into an enforceable contract, we process data as necessary to perform our contracts with you". In part, this legal basis is used "to provide, personalise and improve [...] Meta Products" and to transfer personal data outside the EEA, including to the US. However, the legitimacy of the contract as a lawful basis is subject to scrutiny by regulatory authorities and is currently before the CJEU²²⁵. Meta states that it uses consent to process data provided by "advertisers and other partners" about users' activities outside Meta's products. Consent is also used as a legal basis to collect special category data, to share personal data with advertisers, and to collect information through users' devices (e.g. location). Meta's data policy further states that it uses

²²⁰ This section was written in July 2022 in relation to Meta's policies which were applicable and publicly available at the time. See 'Data Policy' (*Facebook*)

<<https://www.facebook.com/about/privacy/update/printable>> accessed 18 July 2022.

²²¹ See section 1.3.2.6 for more detail on these means of collecting data.

²²² 'Facebook Developer Docs' (*Facebook for Developers*) <<https://developers.facebook.com/docs/>> accessed 7 June 2022.

²²³ 'The Facebook Pixel' (*Meta for Business*) <<https://en-gb.facebook.com/business/learn/facebook-ads-pixel>> accessed 12 May 2022.

²²⁴ 'Data Policy' (*Facebook*) <<https://www.facebook.com/about/privacy/update/printable>> accessed 18 July 2022.

²²⁵ Reference to the Court of Justice of the European Union from the Austrian Supreme Court of Justice (Oberster Gerichtshof) (23 June 2021) 6 Ob 56/21k <https://noyb.eu/sites/default/files/2021-07/Vorlage_sw_EN.pdf>.

the “legitimate interest” legal basis when processing minors' data and for measurement purposes, including to “evaluate the effectiveness of [advertisers' and other partners'] online content and advertising on and off the Meta Company Products”. Meta does not state in the data policy what kind of personal data it collects under the contractual and “legitimate interest” legal bases, or the collection methods used.

Meta also provides tools for individuals to “download” their information, ostensibly in compliance with individuals' rights to access to data, and tools for individuals to port their data to other platforms. For less developed concepts like the right to object, it is unclear how Meta satisfies those rights in practice. For instance, while Meta provides tools to allow users to remove “interest categories” that are used to target adverts, an individual cannot remove those categories entirely. Rather, they are replaced by others.

1.3.3.2 Google's privacy policy

Google's privacy policy²²⁶ confirms that they use “various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs”²²⁷. Although Google's privacy policy includes a definition of some technical terms (e.g. cookies, pixel tags) it has faced legal challenges²²⁸ for allegedly failing to exhaustively set out the purpose for collecting data. Likewise, Google's privacy policy is also subject to legal action for failing to exhaustively explain the legal bases it uses for each data processing purpose.

For example, Google states in the privacy policy that it processes users' information based on consent “for specific purposes” but only provides two examples of those purposes: “to provide you with personalised services, such as ads based on your interests” and “to collect your voice and audio activity for speech recognition”. Google's privacy policy states that it uses the “legitimate interest” legal basis for a variety of non-exhaustive purposes, including to provide non-personalised advertising and to “analyse how people interact with advertising”, but does not stipulate what personal data it collects for these purposes nor how it collects it.

Furthermore, Google's privacy policy notes that they “allow specific partners to collect information from your browser or device for advertising and measurement

²²⁶ This section was written in July 2022 in relation to Google's policies which were applicable and publicly available at the time.

²²⁷ 'Privacy Policy' (Google) <<https://policies.google.com/privacy>> accessed 18 July 2022.

²²⁸ For example, see Ryan J, 'Formal GDPR complaint against Google's internal data free-for-all' (Brave, 16 March 2020) <<https://brave.com/google-internal-data-free-for-all/>> accessed 6 October 2022.

purposes using their own cookies or similar technologies” but does not provide the details of these partners or the categories of data that Google shares with them.

Google’s privacy policy states that where EU law applies, users can “request access to, update, remove, and restrict the processing of their information”. Users can exert their rights to erasure and access under the “exporting & deleting your information” section of Google’s privacy policy.

1.4 Conclusion

Over the past 10-15 years, two companies (Google and Meta) have captured an increasingly large share of digital advertising revenue compared to publishers. Search advertising and social media advertising channels, where large platforms play key roles, have grown at an extremely rapid rate compared to the channel which directs the most advertising revenue to publishers (“other” display). Large platforms have also become key players in the “other” display channel by providing intermediary services for publishers and advertisers to buy and sell ads.

Data plays an essential role in today’s digital advertising market. It is used for targeting and measuring advertising campaigns, often tied to common identifiers that enable companies to build up a picture of an individual’s behaviour across sites, apps, platforms and devices. Large platforms play an important role in this system by controlling the means by which people access the web (e.g. through search, browsers, mobile operating systems and social media) and also through less visible methods (e.g. pixels, fonts) that enable them to embed their data-collecting technology in third-party sites and apps.

The way personal data is collected for digital advertising is changing due to moves by Google and Apple to restrict third-party tracking on their platforms. As a result, many in the industry are focusing on developing new systems and technologies to target and measure ads. In some cases, this involves exploring new ways to identify individuals across different publisher sites and apps, such as shared user IDs. In parallel, Google’s Privacy Sandbox aims to bring together different parts of the advertising industry to develop new solutions which they claim to be more “privacy-preserving” than the status quo. However, this is all still work in progress. The current flux in the industry regarding the way data is collected may present an opportune moment for regulators to identify new ideas and alternative ways of doing digital advertising with less tracking.

2 How has this evolution impacted the privacy of EU citizens, democracy and society in the EU and the environment?

This section provides an overview of a wide range of studies that have looked at the impact of digital advertising on privacy, data protection, democracy, society and the environment. Building on this evidence, it also assesses the available evidence related to the efficacy and efficiency of digital advertising. It concludes by assessing to what extent the potential efficacy and efficiency gains of digital advertising outweigh the societal, privacy and environmental impacts²²⁹.

2.1 Has the evolution of digital advertising led to a high level of privacy and data protection for EU citizens?

Digital advertising has long generated concerns from regulators, individuals and civil society related to privacy and data protection. Numerous GDPR complaints have challenged the legality of the way personal data is processed for digital advertising purposes. A large body of academic work has focused on demonstrating the wider privacy and data protection impacts, including security risks (to individuals and states) and the restriction of individual autonomy over how personal data is collected, shared and used.

2.1.1 Privacy and data protection under the current EU regulatory frameworks

Digital advertising has long generated concerns from regulators and civil society related to privacy and data protection²³⁰. Digital advertising companies operating in the EU must respect European legislation on privacy and data protection,

²²⁹ This section was developed with research, input and drafting provided by Michael Veale.

²³⁰ Millett L I, Friedman B and Felten E, 'Cookies and Web Browser Design: Toward Realizing Informed Consent Online', *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '01* (ACM Press, 2001) <<https://dada.cs.washington.edu/research/tr/2000/12/UW-CSE-00-12-03.pdf>> accessed 19 August 2022.

including the ePrivacy Directive²³¹ and the General Data Protection Regulation (GDPR)²³².

The GDPR contains pertinent obligations on companies involved in the digital advertising ecosystem, such as:

- Any entity processing personal data will need to identify a “legal basis” for that processing. Those legal bases are exhaustively set out in Article 6 GDPR and include the processing of data necessary for the performance of a contract with the user (Article 6.1(b) GDPR), for the purpose of the companies’ legitimate interest (Article 6.1(f) GDPR), or processing data after consent was obtained for a specific purpose (Article 6.1(a) GDPR). How those lawful bases work in practice can be controversial in a digital advertising context and is subject to court and regulatory action. Meta, for example, relies on the contractual legal basis to process personal data for the purpose of personalised advertising. It argues that Facebook’s Terms of Service explicitly refer to ads and sponsored content as being part of the contract with its users²³³. The legitimacy of contracts as a basis for personalised advertising is currently before the European Court of Justice (CJEU) and before regulators. A key consideration is whether personalised advertising can be considered “necessary” for the performance of a social network contract. While many scholars and NGOs disagree²³⁴, the Irish Data Protection Commissioner (DPC) upheld Meta’s interpretation. The matter is now currently being discussed by the European Data Protection Board (EDPB). If the Board disagrees with the decision of the DPC, Facebook will have to rely on another legal basis, such as consent. Likewise, if the CJEU decides that Meta’s reliance on contractual terms is not permissible, Meta will have to provide an alternative lawful basis for processing. Conversely, using legitimate interests as a legal basis under Article 6.1(f) GDPR does not provide data controllers with the unfettered ability to monitor

²³¹ Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11.

²³² 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) OJ L 119, 4.5.2016, p. 1-88.

²³³ See the draft decision of the DPC: ‘Irish DPC Greenlights Facebook’s “GDPR Bypass”.’ (*noyb.eu*, 13 October 2021) <<https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass>> accessed 6 October 2022.

²³⁴ ‘Irish DPC Greenlights Facebook’s “GDPR Bypass”’ (*noyb.eu*, 13 October 2021) <<https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass>> accessed 6 October 2022; Vergnolle S, ‘Why are you on Facebook?’ (*Verfassungsblog*, 1 November 2021) <<https://verfassungsblog.de/why-are-you-on-facebook/>> accessed 6 October 2022.

individuals' behaviour in a digital advertising context. Rather, the context itself provides barriers to reliance on legitimate interests as a legal basis for processing. For example, any monitoring that is done through a particular tracking technology such as cookie deployment would have to meet the requirements for consent in the ePrivacy Directive. Article 6.1(f) GDPR further protects individuals by checking the ability of the controller or third party to rely on "legitimate interests" without first assessing whether the fundamental rights and freedoms of the data subject would override the interests of the controller. Regulatory authorities have cast doubt on whether digital advertising can satisfy that balance²³⁵. These limits reflect the potential intrusion upon subjects' rights posed by some digital advertising data practices.

- The mechanisms that enable digital advertising may require the consent of individuals. Consent has a high bar, requiring the individual to provide a "freely given, specific, informed and unambiguous" indication of their wishes (Article 4.11 GDPR). Consent is also conditional, as laid out in Article 7 GDPR. Despite those high bars, consent is likely to be required for digital advertising, such as when installing cookies on users' devices (Article 5.3 ePrivacy Directive).
- Individuals are given rights over how their data is used in the GDPR, including rights of access and rights to object to processing. However, those rights are often difficult to implement in practice. Given the opacity and complexity of the system, it is difficult for users to identify all the intermediaries and third parties who will receive and process their personal data, which hampers the exercise of their data protection rights. Studies have also shown that the practice and the design of asking for consent through cookie banners can lead to "consent or privacy fatigue", affecting how users behave online²³⁶.
- The Article 29 Working Party suggested that digital advertising can amount to "automated decision making" such that Article 22 GDPR applies. The Working Party argued that digital advertising may be considered as having

²³⁵ See, for example, guidance from the ICO in their report on real-time bidding and the ICO's guidance on digital advertising, as well as guidance from the Article 29 Working Party and the EDPB. 'Update Report into Adtech and Real Time Bidding' (Information Commissioner's Office, 2019) <<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>> and 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Article 29 Data Protection Working Party, 9 April 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.

²³⁶ Choi H, Park J and Jung Y, 'The Role of Privacy Fatigue in Online Privacy Behavior' (2018) 81 *Computers in Human Behavior* 42 <<https://doi.org/10.1016/j.chb.2017.12.001>>.

“significant effect”, for example, when users are targeted using knowledge of their vulnerabilities²³⁷. Other relevant factors to the application of Article 22 include the way an ad is delivered and the intrusiveness of the profiling process²³⁸. In such circumstances, individuals have the right not to be subjected to such automated decisions.

Since the GDPR entered into force, there have been numerous complaints and claims about digital advertising. For instance, claims have been made related to the way consent is collected by websites and platforms in the digital advertising ecosystem. Organisations and studies have highlighted the prevalent use of dark patterns and nudges, especially in the design of cookie banners, which do not clearly offer users the option to refuse consent or nudge users towards consenting²³⁹. As consent must be “informed” and “freely given” many have also questioned whether cookie walls, a barrier that users can only pass if they agree to tracking by third parties, can be considered as valid consent under the GDPR²⁴⁰. That tension with consent requirements is particularly stark as (i) the list of third parties to whom data is passed is impossibly long for individuals to comprehend; and (ii) those third parties pass the data on to yet more third parties who are not identified at the point of collection, meaning any consent could not be “informed” and would in turn be invalid.

There have also been complaints against websites placing tracking cookies even after users clearly object²⁴¹. In one of the earliest GDPR decisions, France’s Commission Nationale Informatique et Libertés (CNIL) ruled against the bundling of consent by a digital advertising company²⁴², where users’ consent was passed

²³⁷ ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679’ (Article 29 Data Protection Working Party, 3 October 2017) <<https://ec.europa.eu/newsroom/article29/items/612053>>.

²³⁸ ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679’ (Article 29 Data Protection Working Party, 3 October 2017) <<https://ec.europa.eu/newsroom/article29/items/612053>>.

²³⁹ See ‘Deceived by Design - How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy’ (Norwegian Consumer Council (Forbrukerrådet), 2018) <<https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>>; Nouwens M and others, ‘Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM, 2020) <<https://dl.acm.org/doi/10.1145/3313831.3376321>> accessed 6 October 2022; Bauer JM, Bergstrøm R and Foss-Madsen R, ‘Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users’ Decisions about Sharing Private Online Data’ (2021) 120 *Computers in Human Behavior* 106729 <<https://www.sciencedirect.com/science/article/abs/pii/S0747563221000510>>.

²⁴⁰ See J Zuiderveen Borgesius F and others, ‘Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation’ (2017) 3 *European Data Protection Law Review* 353 <<https://doi.org/10.21552/edpl/2017/3/9>>.

²⁴¹ ‘Say “NO” to Cookies – yet See Your Privacy Crumble?’ (noyb.eu, 10 December 2019) <<https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble>> accessed 6 October 2022.

²⁴² See: ‘Décision N° MED 2018-042 Du 30 Octobre 2018 Mettant En Demeure La Société X’ (CNIL, 30 October 2018) <<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000037594451/>>.

between companies through contractual relationships. Due to the complexity and opacity of the digital advertising ecosystem, privacy advocates have argued that users are not able to give informed and specific consent, especially when interacting with cookie banners²⁴³. The scale of the issue was highlighted in 2022 by the Belgian data protection authority, Autorité de protection des données (APD), which found that the Transparency and Consent Framework (TCF), developed by IAB Europe and adopted widely across the digital advertising ecosystem, failed to comply with a number of provisions of the GDPR. As well as having an invalid legal basis for the processing and dissemination of users' preferences within the context of the framework, the APD also sanctioned the lack of information provided to users through the interface to allow them to understand the nature and scope of the processing.

2.1.2 Confidentiality

The most widely used digital advertising technologies rely on recording individuals' device, app and web usage²⁴⁴. Some, like display that uses programmatic systems to deliver the ads²⁴⁵, have been alleged to involve the disclosure of this information to thousands of companies²⁴⁶, often without safeguards which ensure the data processed is only used for necessary purposes²⁴⁷.

A 2018 study found that 52 advertising and analytics companies observe more than 91% of users' browsing behaviour on the web. Of these, Google was the most "pervasively embedded around the web"²⁴⁸. According to a 2022 report by the Irish Council for Civil Liberties, personal data is shared 376 times a day on average in Europe as part of programmatic auctions²⁴⁹.

The disclosure of this information can affect privacy and data protection rights. Collecting all of this data makes it vulnerable to disclosure through a data breach.

²⁴³ Matte C, Bielova N and Santos C, 'Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework' (*arXiv*, 21 February 2020) <<http://arxiv.org/abs/1911.09964>> accessed 6 October 2022.

²⁴⁴ See section 1.3.

²⁴⁵ See section 1.1.2.4.

²⁴⁶ 'The Biggest Data Breach' (*Irish Council for Civil Liberties*, May 2022) <<https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe>>.

²⁴⁷ Paragraphs 455 and 472, Belgian Data Protection Authority. (2 February 2022). 'Concerning: Complaint Relating to Transparency & Consent Framework (Decision on the Merits 21/2022 of 2 February 2022)' (Litigation Chamber - Autorité de protection des données, 2 February 2022) <<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>>.

²⁴⁸ Bashir MA and Wilson C, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) 4 2018 Proceedings on Privacy Enhancing Technologies 85 <<https://doi.org/10.1515/popets-2018-0033>>.

²⁴⁹ 'The Biggest Data Breach' (*Irish Council for Civil Liberties*, May 2022) <<https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe>>.

Partly owing to the lack of aggregate data on the number of cyberattacks that have resulted from advertising-related data leaks, it is difficult to measure the extent to which data collected and disclosed for digital advertising purposes risks exposure through data breaches. However, several high-profile examples highlight impacts on privacy and data protection rights as a cause for significant concern. In 2020, TechCrunch reported that Oracle's BlueKai data management platform (DMP) exposed "billions" of user records from online tracking infrastructures, including names, email and home addresses, purchases, newsletter subscriptions and web browsing data²⁵⁰. Similar recent exposures of data from other data brokers have been characterised as revealing the data of hundreds of millions of individuals²⁵¹.

Data on individuals can be made available on the open market, posing a potential security risk and creating opportunities for people's information to be weaponised against them.

- In 2021, religious publication The Pillar used commercially available data to publicly expose the sexual orientation of a priest. This data appears to be sourced from digital advertising intermediaries observing behaviour related to the dating app Grindr²⁵².
- The US military has reportedly purchased location data from Babel Street and X-Mode. These companies use trackers embedded in software (e.g. Muslim prayer apps, spirit-level measurement apps) to "draw a shape on a map, see all devices [the tracker firm] has data on in that location, and then follow a specific device around to see where else it has been"²⁵³.
- As part of their border-enforcement activities, the US Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) agencies have reportedly purchased location data initially collected by

²⁵⁰ Whittaker Z, 'Oracle's BlueKai Tracks You across the Web. That Data Spilled Online' (*TechCrunch*, 19 June 2020) <<https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/>> accessed 12 May 2022.

²⁵¹ Ikeda S, 'Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak' (*CPO Magazine*, 28 August 2020) <<https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/>> accessed 12 May 2022.

²⁵² O'Brien M and Bajak F, 'Priest Outed via Grindr App Highlights Rampant Data Tracking' (*ABC News*, 22 July 2021) <<https://abcnews.go.com/Business/wireStory/priest-outed-grindr-app-highlights-rampant-data-tracking-78993991>> accessed 15 June 2022.

²⁵³ Cox J, 'How the U.S. Military Buys Location Data from Ordinary Apps' (*Vice*, 16 November 2020) <<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>> accessed 12 July 2022.

mobile phones and apps for digital advertising purposes via government contractor Venntel²⁵⁴.

- Concerns have been raised about data collected by Russian platform Yandex, whose CEO became the target of EU sanctions in March 2022 in connection with Russia's invasion of Ukraine²⁵⁵. Industry experts have noted that Yandex software development kits (SDKs)²⁵⁶ collect individuals' data as part of the permissions that users provide to a large variety of apps (including messaging apps, games, Virtual Private Networks (VPNs) and location-sharing tools) and that this data may be stored in Russia²⁵⁷. Additionally, concerns have been raised about the presence of cookies provided by Yandex on European websites²⁵⁸. Researcher Zach Edwards has suggested that "for people with a high-threat profile or working in high-profile jobs, using apps that send this data to Moscow is dangerous and can potentially lead to attacks on home networks or other forms of digital surveillance"²⁵⁹.
- According to the CJEU's Schrems II ruling, US national legislation does not sufficiently restrict local authorities' ability to access personal data transferred from the EU²⁶⁰. This means that personal data transferred to the US as part of digital advertising could be accessed by US authorities. The privacy policies of various US-based digital advertising intermediaries

²⁵⁴ Tau B, 'Federal Agencies Use Cellphone Location Data for Immigration Enforcement' (*Wall Street Journal*, 7 February 2020) <<https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>> accessed 3 June 2022; and Cox J, 'How an ICE Contractor Tracks Phones Around the World' (*Vice*, 3 December 2020) <<https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps>> accessed 3 June 2022.

²⁵⁵ Yandex CEO Tigran Oganessian has since resigned from his position. See RFI, 'Head of Russia's Yandex resigns after being hit by EU sanctions' (*RFI*, 16 March 2022) <<https://www.rfi.fr/en/head-of-russia-s-yandex-resigns-after-being-hit-by-eu-sanctions>> accessed 27 May 2022.

²⁵⁶ See section 1.3.1.1.2.

²⁵⁷ McGee P, 'Russian tech giant Yandex's data harvesting raises security concerns' (*Financial Times*, 29 March 2022) <<https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb>> accessed 27 May 2022.

²⁵⁸ Dehaye P, '@Anouch de @LeTemps écrit sur le cauchemar que sont les traceurs dans différentes apps. "Une histoire sans fin"...' (*Twitter*, 10 April 2022) <<https://twitter.com/podehaye/status/1513199620129792005>> accessed 27 May 2022.

²⁵⁹ For an overview of the risks of interception of personal data by Russian government entities and the underlying legal framework, see also 'Government access to data in third countries' (*European Data Protection Board*, 2019, p.40-52) <https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf>.

²⁶⁰ According to the CJEU's Schrems II ruling, US surveillance programmes, as implemented by the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, "are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter." Case C-311/18 (Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, 2020) <<https://curia.europa.eu/juris/liste.jsf?num=C-311/18>>.

suggest that they may transfer EU residents' personal data to the US²⁶¹. That said, it is not clear whether they have put in place safeguards against access by US authorities, as mandated by the Schrems II ruling²⁶². The Austrian and French data protection authorities have both issued decisions stating that the safeguards put in place by Google for Google Analytics were not compliant with the Schrems II ruling²⁶³. Meta's compliance with the Schrems II ruling is the subject of an investigation by the Irish data protection authority²⁶⁴.

Data that is for sale is likely only the tip of the iceberg, as more sophisticated cyber-attacks may be undertaken by criminal groups or foreign state actors against digital advertising infrastructures to exfiltrate confidential data on individuals and their technology usage patterns. The covert nature of these operations, and the advanced nature of hacking tools, which are often designed to leave no trace, mean we know little about the scale of this practice other than recognising that digital advertising firms represent an attractive target for those seeking bulk datasets. In the case of a 2017 hack that involved stealing data from data broker Equifax – which claims to have data on digital targeting segments, wealth, financial durability, auto, income, credit card spending propensities, business to business activities, mortgages, financial mobility, online interests, financial cohorts, investments, insurance, credit cards, student loans, retail banking, small business assets, restaurants, ability to pay, communications, travel

²⁶¹ For example, see: 'Google Ads Processing Terms' (*Google*) <<https://business.safety.google/adsprocessor/terms/>> accessed 1 July 2022; 'Privacy Notice' (*DoubleVerify*) <<https://doubleverify.com/privacy-notice/>> accessed 1 July 2022; 'Privacy Policy' (Oracle) <<https://www.oracle.com/be/legal/privacy/privacy-policy.html>> accessed 1 July 2022; 'Privacy Policy' (*Sizmek*) <<https://www.sizmek.com/privacy-policy/>> accessed 1 July 2022; 'Platform Privacy Policy' (*Xandr*); <https://xandr.com/privacy/platform-privacy-policy/#where_operate> accessed 1 July 2022; 'Advertising Technology Privacy Policy' (*Magnite*) <<https://www.magnite.com/legal/advertising-technology-privacy-policy/>> accessed 1 July 2022.

²⁶² For an overview of the safeguards entities should put in place when transferring personal data to third countries that do not have data protection laws equivalent to the EU's, see 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf>.

²⁶³ See 'Bekanntmachungen der Datenschutzbehörde: Information der Datenschutzbehörde zur Entscheidung über die Verwendung von Google Analytics' (*Datenschutzbehörde*, 13 January 2022) <<https://www.dsb.gv.at/download-links/bekanntmachungen.html>> accessed 1 July 2022; and 'Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply' (*Commission nationale de l'informatique et des libertés*, 10 February 2022) <<https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>> accessed 1 July 2022.

²⁶⁴ See Manancourt V, 'Europe Faces Facebook Blackout' (*Politico*, 7 July 2022) <<https://www.politico.eu/article/europe-faces-facebook-blackout-instagram-meta-data-protection/>> accessed 11 July 2022.

and leisure, sports, and more — US authorities indicted four individuals working for the Chinese military as responsible for the hack²⁶⁵.

Beyond undermining confidentiality, several scholars have argued that harms to privacy could also be detrimental to users' autonomy and self-determination. In essence, they argue that individuals may modify their behaviour in response to a lack of privacy, which can effectively hinder their ability to self-realise, grow and develop. As Rouvroy and Pouillet note, privacy can be conceived as a form of "informational self-determination", whereby "an individual's control over the data and information produced about him is a [...] precondition for him to live an existence that may be said [to be] 'self-determined'"²⁶⁶. In the context of advertising, Cohen has further argued that because digital advertising infrastructures enable individuals' activities to be tracked and made technically accessible, "we are losing the ability to control the processes of personalised shaping or even to know much about them"²⁶⁷. Importantly, here she draws attention not to information on the individual movements of data points, but to knowledge about processes of personalisation — what is delivered, to whom, when, and what effect it has on that individual's "configuration" of themselves in an increasingly complex, networked environment. This draws attention to the outcomes of profiling, targeting and commodification of attention, rather than simply the process, which today largely involves the data collection referred to above. Issues with self-realisation and related challenges could still create the same or similar problems, even where systems move to "privacy-friendly" approaches (such as the proposed on-device targeting in Google's Privacy Sandbox)²⁶⁸ as these technologies tend to only focus on confidentiality issues related to sharing data with multiple third parties.

2.1.3 Vector for state surveillance

A particular type of impact on privacy and data protection rights relates to how the features of digital advertising systems designed to uniquely identify users can, and have been, piggybacked on by state actors to monitor internet traffic for the purposes of intelligence. With the exception of leaks from whistleblowers, the clandestine nature of state surveillance precludes the availability of data to evaluate its relationship with digital advertising. Nevertheless, the use of

²⁶⁵ Benner K, 'U.S. Charges Chinese Military Officers in 2017 Equifax Hacking' (*New York Times*, 10 February 2020) <<https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html>> accessed 7 June 2022.

²⁶⁶ Chapter 10 of Rouvroy A and Pouillet Y, *Reinventing Data Protection?* (Springer, 2009) <https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_2>.

²⁶⁷ See Chapter 8 of: Cohen JE, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012) <<http://juliecohen.com/configuring-the-networked-self>>.

²⁶⁸ See sections 1.3.1.2.2 and 5.2.

advertising as a vector for state surveillance has been documented in practice, as well as the potential highlighted in theoretical and empirical studies.

Soltani et al. analysed documents released by whistleblower Edward Snowden to illustrate the ways in which security agencies used uniquely identifying Google PREF cookies to single out a user's computer and allow it to be remotely exploited using tools developed by state actors²⁶⁹. Further Snowden documents released by The Guardian indicate the role that Google DoubleClick cookies have had in techniques to re-identify users of the Tor Browser, a widely used technique for anonymous internet access relied on by NGOs, journalists and civil society activists around the world²⁷⁰. Englehardt et al. conclude that "third-party tracking cookies enable an adversary to attribute traffic to users much more effectively than methods such as considering IP address alone"²⁷¹. Vanrykel et al. show similar findings related to digital advertising tools in mobile applications²⁷². Papadopoulos et al. find that the "cookie synchronisation" method deployed by companies to share user details with each other for digital advertising purposes can be used to leak the identities of individuals to third parties²⁷³.

2.1.4 Loss of rights and control

Helberger et al. note that "while consumers historically have accepted advertising as a means to get free or discounted access to mass media content, the loss of control over personal data and privacy was not considered a part of the deal"²⁷⁴. Control in this sense is an integral part of the fundamental right to data protection, as this right provides "infrastructure that regulates disproportionate power in an attempt at safeguarding" values such as autonomy, freedom, and human dignity. Part of this are the individual rights given to data subjects, such as rights to access and erasure, which are enshrined in legislation such as the GDPR; but the broader

²⁶⁹ Soltani A and others, 'NSA Uses Google Cookies to Pinpoint Targets for Hacking' (*Washington Post*, 10 December 2013) <<https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>> accessed 7 June 2022.

²⁷⁰ "'Tor Stinks' Presentation - Read the Full Document' (*The Guardian*, 4 October 2013) <<http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>> accessed 11 July 2022.

²⁷¹ Englehardt S and others, 'Cookies That Give You Away: The Surveillance Implications of Web Tracking', *Proceedings of the 24th International Conference on World Wide Web* (International World Wide Web Conferences Steering Committee, 2015) <<https://dl.acm.org/doi/10.1145/2736277.2741679>> accessed 11 July 2022.

²⁷² Vanrykel E and others, 'Leaky Birds: Exploiting Mobile Application Traffic for Surveillance' in Jens Grossklags and Bart Preneel (eds), *Financial Cryptography and Data Security*, vol 9603 (Springer Berlin Heidelberg, 2017) <http://link.springer.com/10.1007/978-3-662-54970-4_22> accessed 11 July 2022.

²⁷³ Papadopoulos P, Kourtellis N and Markatos EP, 'Exclusive: How the (Synced) Cookie Monster Breached My Encrypted VPN Session', *Proceedings of the 11th European Workshop on Systems Security* (ACM, 2018) <<https://dl.acm.org/doi/10.1145/3193111.3193117>> accessed 8 July 2022.

²⁷⁴ Helberger, N and others, 'Macro and exogenous factors in computational advertising: Key issues and new research directions.' *Journal of Advertising* (2020), 49(4), 377-393, p. 381.

Charter rights relate to architectures of control — ensuring that as a whole, the data economy does not become uncontrollable²⁷⁵.

Aspects of the way digital advertising functions today can make it very difficult for users to exercise legal rights, such as rights to access, erasure or objection to data processing. This is particularly evident in programmatic display advertising, which utilises data collected by multiple third parties across websites and apps. Consent management systems have been shown to include tracking requests from a median 315 different digital advertising intermediaries²⁷⁶. This high number relates both to the large number of trackers on the web and in apps, but also to the complex ways data is transmitted between organisations on the server-side²⁷⁷, and the legal links between which organisations control and own which tracking infrastructures^{278, 279}. This makes it difficult for a user to identify which organisations hold data that relates to them. Furthermore, the focus on identifiers in digital advertising makes it very hard for users to exercise their rights of access, because they are often not able, either due to lack of transparency or technical and legal barriers, to access and prove the provenance of the identifiers connected to them^{280, 281}. Kroger et al. found that a majority of mobile app providers they contacted provided no or insufficient responses to data access requests, for example²⁸².

When users do manage to exercise these rights, they can find a surprising amount of data being collected. In the case of Quantcast, a week of data consisted for one

²⁷⁵ Ausloos J, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection* (1st ed.) (Oxford University Press, 2020), p. 61-62.

²⁷⁶ Nouwens M and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM, 2020), p. 5, <<https://dl.acm.org/doi/10.1145/3313831.3376321>> accessed 8 August 2022.

²⁷⁷ Bashir MA and Wilson C, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) 2018 Proceedings on Privacy Enhancing Technologies 85, <https://www.researchgate.net/publication/327994246_Diffusion_of_User_Tracking_Data_in_the_Online_Advertising_Ecosystem>.

²⁷⁸ Binns R and Bietti E, 'Acquisitions in the Third Party Tracking Industry: Competition and Data Protection Aspects' [2018] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3269473>> accessed 12 August 2022.

²⁷⁹ Binns R and others, 'Measuring Third-Party Tracker Power across Web and Mobile' (2018) 18 ACM Transactions on Internet Technology 1 <<https://dl.acm.org/doi/10.1145/3176246>>.

²⁸⁰ Norval C and others, 'RECLAIMING Data: Overcoming App Identification Barriers for Exercising Data Protection Rights', *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (ACM, 2018) <<https://dl.acm.org/doi/10.1145/3267305.3274153>> accessed 12 August 2022.

²⁸¹ Veale M, Binns R and Ausloos J, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105, <<https://academic.oup.com/idpl/article/8/2/105/4960902>>.

²⁸² Kröger JL, Lindemann J and Herrmann D, 'How Do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on IOS and Android Apps', *Proceedings of the 15th International Conference on Availability, Reliability and Security* (ACM, 2020) <<https://dl.acm.org/doi/10.1145/3407023.3407057>> accessed 12 April 2022.

data subject of “5,300 rows and more than 46 columns worth of data including URLs, time stamps, IP addresses, cookie IDs, browser information and much more”²⁸³. Data broker Iovation was found to hold more than 19,000 attributes related to one data subject in a recent investigation into personal data shared by gambling websites²⁸⁴.

The impact of the practical loss of rights was further highlighted in a recent ruling by the APD concerning the GDPR compliance of real-time bidding and programmatic advertising using IAB Europe’s widely adopted TCF. This has been highlighted as a challenge which is structurally difficult to remedy given the technical functionality of the ecosystem²⁸⁵.

More broadly, digital advertising data infrastructures can make it hard for users to understand how and where their personal data is collected. This is illustrated through studies where individuals misunderstand features in their browser like Incognito Mode or Private Windows, believing that they prevent companies from tracking their activity when this is not the case²⁸⁶. Though using a relatively small sample size, a study by Abu-Salma and Livshits found that “almost all participants did not understand the security goal of private browsing” with most “incorrectly believing their browsing or search history would get deleted from Google’s records after exiting private mode”²⁸⁷. Complex and persistent tracking techniques such as fingerprinting make it hard for users to understand how the web works in relation to privacy and confidentiality²⁸⁸.

A 2019 report found that while a majority (63%) of individuals supported the way digital advertising worked when initially asked, once a brief explanation of its functioning was provided, acceptability fell to just 36%²⁸⁹. Even where consumers

²⁸³ Kaltheuner F, ‘I Asked an Online Tracking Company for All of My Data and Here’s What I Found’ (*Privacy International*, 7 November 2018) <<https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>> accessed 12 May 2022.

²⁸⁴ Christl W, ‘Digital Profiling in the Online Gambling Industry’ (*Cracked Labs*, 2022) <<https://cdn.sanity.io/files/btrscf0/production/e23ea75fe93f775d9f9ed795427f4b5ed8d67016.pdf>>.

²⁸⁵ Veale M, Nouwens M and Santos C, ‘Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?’ [2022] *Technology and Regulation* 12, p. 18-20, <<https://techreg.org/article/view/11594>>.

²⁸⁶ Abu-Salma R and Livshits B, ‘Evaluating the End-User Experience of Private Browsing Mode’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM, 2020), p. 7, <<https://dl.acm.org/doi/10.1145/3313831.3376440>> accessed 12 May 2022.

²⁸⁷ Abu-Salma R and Livshits B, ‘Evaluating the End-User Experience of Private Browsing Mode’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM, 2020), p. 7, <<https://dl.acm.org/doi/10.1145/3313831.3376440>> accessed 12 May 2022.

²⁸⁸ Acar G and others, ‘The Web Never Forgets: Persistent Tracking Mechanisms in the Wild’, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, 2014) <<https://dl.acm.org/doi/10.1145/2660267.2660347>> accessed 12 May 2022.

²⁸⁹ Worledge M and Bamford M, ‘Adtech Market Research Report’ (*Ofcom*, 21 March 2019) <https://www.ofcom.org.uk/data/assets/pdf_file/0023/141683/ico-adtech-research.pdf> accessed 12 May 2022.

do suspect certain tracking methods are technically possible, such as third parties recording web browsing history, research has long indicated their expectations are often below real usage²⁹⁰. Where advertising explanations are given by platforms, users typically find them incomplete and unsatisfactory compared to the underlying targeting mechanisms²⁹¹.

2.2 What impact has the evolution of digital advertising had on democracy and society in the EU?

Digital advertising is most commonly targeted based on known or inferred information about individuals, rather than the place where the ad will be displayed. This feature of the market is exploited by actors who profit from ads sold next to content which is harmful to democracy and society, such as disinformation. Digital advertising can also be used to spread harmful content and amplify discrimination through ad content and manipulation of ad targeting methods.

2.2.1 Harmful content

Digital advertising can serve as a vector for a variety of content that is harmful in a range of societally impactful ways. Information of this type can be both presented *in* ads, as well as *alongside* them, and is facilitated by the ability to monetise this content easily through indirect ad delivery mechanisms like programmatic advertising. Analysis by The Global Disinformation Index estimates that \$235 million is paid annually through advertising to the 20,000 disinformation sites listed on their database²⁹².

2.2.1.1 Disinformation and harmful content in ads

Consumer groups note that it is easy to send out fake health advice and advertise non-existent brands using digital advertising channels, highlighting the risk of

²⁹⁰ Ur B and others, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising', *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (ACM Press, 2012) <<http://dl.acm.org/citation.cfm?doid=2335356.2335362>> accessed 12 May 2022.

²⁹¹ Wei M and others, 'What Twitter Knows: Characterizing Ad Targeting Practices, User Perceptions, and Ad Explanations Through Users' Own Twitter Data', *29th USENIX Security Symposium (USENIX Security 20)* (USENIX Association, 2020) <<https://www.usenix.org/conference/usenixsecurity20/presentation/wei>>.

²⁹² 'The Quarter Billion Dollar Question: How Is Disinformation Gaming Ad Tech?' (*The Global Disinformation Index*, 1 September 2019) <<https://www.disinformationindex.org/>> accessed 6 October 2022.

such “scam ads” to the general public²⁹³. Public figures have found their images and personalities abused in digital ads to promote financial products and have struggled to hold the original advertisers to account²⁹⁴ even though these actions would not just breach personality rights but would often be manifestly illegal under the Unfair Commercial Practices Directive²⁹⁵. Zeng et al. studied “problematic” ads in the programmatic display ecosystem, finding that the majority of those they surveyed were perceived badly by users for a variety of reasons, including perceptions of them as clickbait, untrustworthy, or distasteful²⁹⁶. The study provides empirical support for the scale of harmful and deceptive advertising, finding 44.6% of ads they surveyed to be “problematic”, including 16.9% of Google-served ads²⁹⁷.

2.2.1.2 Disinformation and harmful content alongside ads

Programmatic advertising has created incentives for actors to create websites that are designed to monetise engagement with content by exploiting the use of techniques which place ads based on information about the individual likely to be viewing them, rather than the environment the ads will appear in. This disconnects advertisers and their agencies from the content ads are placed next to, creating opportunities for advertising spend to flow to harmful content, including disinformation²⁹⁸. Braun and Eklund describe how digital advertising infrastructures create a “lucrative incentive structure for ‘fake news’ publishers”²⁹⁹. In some cases, data about individuals can be used to target them

²⁹³ Laughlin A, ‘Fake Ads; Real Problems: How Easy Is It to Post Scam Adverts on Facebook and Google?’ (*Which? News*, 6 July 2020) <<https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/>> accessed 11 May 2022.

²⁹⁴ Hern A, ‘Martin Lewis Drops Lawsuit as Facebook Backs Scam Ads Scheme’ (*The Guardian*, 23 January 2019) <<https://www.theguardian.com/technology/2019/jan/23/martin-lewis-drops-lawsuit-as-facebook-backs-scam-ads-scheme>> accessed 11 May 2022.

²⁹⁵ 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’).

²⁹⁶ Zeng E, Kohno T and Roesner F, ‘Bad News: Clickbait and Deceptive Ads on News and Misinformation Websites’ [2020] Workshop on Technology and Consumer Protection (ConPro), p. 11, <<https://www.ieee-security.org/TC/SPW2020/ConPro/papers/zeng-conpro20.pdf>>.

²⁹⁷ The definition of “problematic” used in the Zeng et al. study is outlined in their study’s appendix. It includes ads from content farms, misleading insurance advertorials encouraging users to disclose personal data, ads for non-FDA approved supplements, “potentially unwanted software”, among other categories of misleading or harmful ads.

²⁹⁸ Melford C and Fagan C, ‘Cutting the Funding of Disinformation: The Ad-Tech Solution’ (*The Global Disinformation Index*, May 2019) <https://disinformationindex.org/wp-content/uploads/2019/05/GDI_Report_Screen_AW2.pdf> accessed 16 May 2022.

²⁹⁹ Braun JA and Eklund JL, ‘Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism’ (2019) 7 *Digital Journalism* 1, <<https://www.tandfonline.com/doi/abs/10.1080/21670811.2018.1556314?journalCode=rdij20>>.

on “cheaper” websites that spread disinformation instead of premium publisher sites³⁰⁰.

Concerns have also been raised about the digital advertising industry’s response to Russia’s invasion of Ukraine. A report by Adalytics found that Google ad exchanges were serving ads from large advertisers on websites that have been the target of US sanctions, or which operate from countries that have been the target of US sanctions³⁰¹. Some of these websites have also been the target of EU sanctions³⁰². This issue has also been observed on Google’s own platforms. For example, journalist Mark Scott discovered that YouTube channels posting disinformation about Russia’s invasion of Ukraine continued to generate revenue through ads³⁰³.

As Adalytics points out, Google took several steps as a response to Russia’s invasion of Ukraine, including pausing the “monetisation of content that exploits, dismisses, or condones the war”³⁰⁴. Furthermore, although Adalytics was able to observe ads being displayed on sanctioned websites, the researchers acknowledge being unable to verify whether brand safety controls prevented the advertisers from being charged for the associated transactions and the websites in question from being remunerated. The report notes that ads from large advertisers may have appeared on sanctioned websites without the advertisers’ knowledge, in part because Google allows a majority of publishers and intermediaries using its exchanges to remain anonymous³⁰⁵. Researchers have nonetheless continued to observe websites that condone the war in Ukraine being monetised through

³⁰⁰ Ryan J, ‘The Adtech Crisis and Disinformation’ (2019) <<https://www.slideshare.net/JohnnyRyan/the-adtech-crisis-and-disinformation>> accessed 16 May 2022.

³⁰¹ ‘Are Google’s ad exchange & Fortune 500 advertisers working with Treasury sanctioned websites in Russia, Iran, & Syria?’ (*Adalytics*, 2022) <<https://adalytics.io/blog/adtech-sanctions>> accessed 26 May 2022.

³⁰² See for instance websites owned by VK Company, whose CEO became the target of EU sanctions in March 2022. See Council Regulation 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, OJ L 078 17.3.2014.

³⁰³ Scott M, ‘Digital Bridge: Russians ads — Covid anniversary — US state privacy’ (*Politico*, 10 March 2022) <<https://www.politico.eu/newsletter/digital-bridge/russians-ads-covid-anniversary-us-state-privacy/>>, accessed on 14 July 2022.

³⁰⁴ For an overview of other measures that large platforms and digital advertising intermediaries have taken in response to Russia’s invasion of Ukraine, see Rakowitz R, ‘Ukraine: Taking action on digital advertising’ (*World Federation of Advertisers*, 31 March 2022) <<https://wfanet.org/knowledge/item/2022/03/31/Ukraine-Taking-action-on-digital-advertising>> accessed 27 May 2022.

³⁰⁵ ‘Are Google’s ad exchange & Fortune 500 advertisers working with Treasury sanctioned websites in Russia, Iran, & Syria?’ (*Adalytics*, 2022) <<https://adalytics.io/blog/adtech-sanctions>> accessed 26 May 2022.

Google's intermediary services³⁰⁶. Indeed, NewsGuard, an organisation that rates the credibility of news and information websites, identified "more than two dozen websites" that were generating revenue through Google Ads while hosting disinformation about Russia's invasion of Ukraine³⁰⁷ despite the steps taken by Google to remedy this issue.

The advertising industry has characterised this issue as "brand safety", due to the perceived reputational risk of ads appearing next to content which is not perceived to be appropriate to the brand being advertised. In some cases, this could be because the content is harmful or illegal; in others, it could be brand-specific, for example ads for an airline appearing next to content about plane crashes. Large platforms and intermediaries have responded to this by providing "brand safety controls" for advertisers, as well as designing blanket monetisation policies to prevent certain types of content (e.g. disinformation, voter fraud) having ads served next to them. However, there is evidence that these controls and policies are not entirely effective in preventing ads from appearing next to harmful content. In 2018, Sizmek (acquired by Amazon in 2019) found that 64% of advertisers found it difficult to implement brand safety controls related to harmful content and disinformation³⁰⁸. In 2019, advertisers using Google Ads complained of being unable to prevent their ads from being served in countries that were subject to sanctions by the US Office of Foreign Assets Control at the time, including Iran, North Korea and Syria³⁰⁹. An analysis by The Global Disinformation Index found that 25% of the large platforms and intermediaries they studied were displaying ads next to content that violated their own policies³¹⁰.

The digital advertising industry, particularly advertisers, have raised concerns about advertising being placed next to, and therefore used to fund, harmful content³¹¹. The EU's Strengthened Code of Practice on Disinformation (the Code) aims to contribute to resolving these issues. Effective from January 2023, it will require that its signatories (including large platforms, advertisers, and

³⁰⁶ 'Are Google's ad exchange & Fortune 500 advertisers working with Treasury sanctioned websites in Russia, Iran, & Syria?' (*Adalytics*, 2022) <<https://adalytics.io/blog/adtech-sanctions>> accessed 27 May 2022.

³⁰⁷ Skibinski M, 'Despite Promises, Google and Other Ad Platforms Are Still Funding Russian Disinformation' (*NewsGuard*, 7 March 2022) <<https://www.newsguardtech.com/special-reports/ads-russian-propaganda/>> accessed on 14 July 2022.

³⁰⁸ Sizmek, 'Marketers Survey Results 2018: An Insider's Look at Media, Brand Safety, and Partnerships' (*Sizmek*, 2018) <http://digitaltransmedia.digitaltransformers.cat/wp-content/uploads/2018/09/Marketers_Survey_2018.pdf>.

³⁰⁹ Lapowsky I, 'When Google Serves Ads in Iran, Advertisers Pay the Price' (*Wired*, 15 May 2019) <<https://www.wired.com/story/google-ads-sanctioned-countries-iran/>> accessed 25 May 2022.

³¹⁰ 'Ad Tech Policy and Enforcement Gaps: Challenges and Solutions' (*The Global Disinformation Index*, 2022) <<https://www.disinformationindex.org/research/2022-09-07-ad-tech-policy-and-enforcement-gaps-challenges-and-solutions/>>.

³¹¹ See, for example, the Global Alliance for Responsible Media 'About GARM' (*World Federation of Advertisers*) <<https://wfanet.org/leadership/garm/about-garm>> accessed 25 May 2022.

intermediaries) commit to “defund the dissemination of disinformation”³¹². Commitments under the Code include avoiding the publication of disinformation, preventing ads from appearing next to disinformation, informing advertisers about where their ads are placed, promoting the use of brand safety tools, and providing data to third-party auditors on the effectiveness of measures taken under the Code. Given its voluntary nature, the Code’s effectiveness will depend on signatories’ willingness to implement it³¹³ and the companies that agree to sign up to it. As of July 2022, although Google and Meta are signatories, just three intermediaries have signed up to the Code, although IAB Europe is a signatory³¹⁴. Additionally, although their representative trade association (the World Federation of Advertisers) is a signatory, no advertiser has signed up to the Code. The Digital Services Act’s (DSA) provisions on risk assessments and risk mitigation measures may encourage the implementation of the Code³¹⁵.

2.2.2 Discrimination

Digital advertising has been shown to facilitate discrimination by selecting or excluding target audiences based on categories that are protected under equality law. Meta was alleged to have permitted advertisers to exclude target audiences of housing and employment ads by ethnicity and “ethnic affinity”, a practice prohibited under US federal law³¹⁶. Google was likewise said to have allowed

³¹² ‘The 2022 Code of Practice on Disinformation’ (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>> accessed 12 July 2022.

³¹³ Indeed, the European Commission’s assessment of the original Code of Practice on Disinformation noted the “inconsistent and incomplete application of the Code across platforms and Member States”. See European Commission Staff Working Document: Assessment of the Code of Practice on Disinformation - Achievements and Areas for Further Improvement, SWD(2020) 180, <<https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement>>.

³¹⁴ ‘Signatories of the 2022 Strengthened Code of Practice on Disinformation’ (*European Commission*, 16 June 2022) <<https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>>, accessed 15 July 2022.

³¹⁵ Article 34 DSA will require “very large online platforms” (likely to include Google and Meta) to assess the presence of systemic risks on their services, including those relating to disinformation. Article 35 DSA will require them to take measures to mitigate those risks, including through their digital advertising services. The Code of Practice on Disinformation may therefore be used to assess the application of Articles 34 and 35 DSA when it comes to disinformation. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

³¹⁶ Angwin J, Tobin A and Varner M, ‘Facebook (Still) Letting Housing Advertisers Exclude Users by Race — ProPublica’ (*ProPublica*, 21 November 2017) <<https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin>> accessed 15 June 2022; Angwin J and Parrish Jr T, ‘Facebook Lets Advertisers Exclude Users by Race’ (*ProPublica*, 28 October 2016) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race?token=EnKC07S5tur0EVV_U9AOINE-b5icIEOw> accessed 12 July 2022.

advertisers to discriminate against women³¹⁷ and nonbinary people³¹⁸ using targeting criteria for job ads. Standard industry tools to categorise and target audiences for display advertising would characterise users' browsing history explicitly by sexuality, religious and political views, and health status³¹⁹, which could be used to discriminate against users. The latter approach illustrates a difficulty in restricting this type of functionality for any system where browsing history can form part of targeting criteria, as pages that are closely linked to topics or communities can likely be used to construct effective estimates for protected characteristics.

According to Speicher et al., advertisers using Facebook can use criteria to target users based on characteristics implied by different interest categories, sometimes in a discriminatory fashion³²⁰. Facebook's ban on targeting based on protected characteristics such as ethnicity has not been able to counter this use of proxies. The study found that large numbers of non-sensitive attributes for targeting ads on Facebook seemed to correlate with protected characteristics as defined under equality law and, in turn, those attributes could be used to create highly discriminatory ad targeting. Venkatadri and Mislove study this issue further, noting how even when Facebook adds extra controls to prevent attributes or interests with skewed distribution being used to discriminate, advertisers can use compositions of attributes to achieve the same effect³²¹. They conclude that this is a very difficult practice to defend against as it remains possible even if all highly skewed attributes are removed from the interface.

2.2.2.1 "Lookalike Audiences"

Certain advertising services are able to use lists of identified people and certain other criteria (such as geographic scope) to target audiences of users who are similar (by some proprietary definition of similarity) to the original list³²². Speicher et al. suggest that Facebook's "lookalike audience" feature could amplify both

³¹⁷ Datta Amit, Tschantz M C and Datta Anupam, 'Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination' (2015) 1 Proceedings on Privacy Enhancing Technologies 92-112 <<https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf>>.

³¹⁸ Merril J B, 'Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads' (*The Markup*, 11 February 2021) <<https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads>> accessed 8 June 2022.

³¹⁹ 'RTB Online Ad Auctions' (*Irish Council for Civil Liberties*) <<https://www.iccl.ie/rtb/>> accessed 6 October 2022.

³²⁰ Speicher T and others, 'Potential for Discrimination in Online Targeted Advertising' in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR, 2018) <<https://proceedings.mlr.press/v81/speicher18a.html>>.

³²¹ Venkatadri G and Mislove A, 'On the Potential for Discrimination via Composition', *Proceedings of the ACM Internet Measurement Conference* (ACM, 2020) <<https://dl.acm.org/doi/10.1145/3419394.3423641>> accessed 15 August 2022.

³²² Facebook and Twitter run "lookalike audiences"; Google run "similar audiences"; Pinterest runs "actalike audiences".

intentional and unintentional skews introduced in the initial “source audience” from which the broader targeted audience is generated, leading to discriminatory effects^{323, 324}.

Assessing the extent to which advertisers use these features to discriminate against minority groups is challenging, particularly in the absence of data. However, studies suggest that “in employment, housing, lending, and other aspects of life, racial proxies such as one’s name and neighbourhood can increase the degree to which human decision-makers discriminate”³²⁵. Zang suggests that Facebook’s “African-American Culture” targeting option became significantly more accurate in reaching nearly the same number of African American users than its “African American (US)” option, which it removed. Additionally, they found that “lookalike audience based on Asian voters with commonly-given Asian names and who live in popular Asian ZIP codes had a sample share of 100% Asians”. This suggests that digital advertising could act as a vehicle for discrimination by allowing advertisers to target ads for key services to, or exclude, specific ethnic groups.

2.2.2.2 Economic origins of indirect discrimination in digital advertising

A range of other studies show how pricing attention using online markets can bring indirectly discriminatory effects. Lambrecht and Tucker attribute differences in the way employment-related ads are shown to men and women to the higher cost of advertising to young women³²⁶. They argue that this creates disparate ad delivery

³²³ Speicher T and others, ‘Potential for Discrimination in Online Targeted Advertising’ in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR, 2018) <<https://proceedings.mlr.press/v81/speicher18a.html>>.

³²⁴ As part of a lawsuit settlement, Facebook created “Special Ad Audiences”, which is the only form of lookalike audiences available when organisations try to target housing, credit and employment ads, all of which are subject to heightened US federal regulation. Sapiezynski et al. present evidence that this new functionality does not reduce bias in the targeted audience among race, age or gender lines compared to the original feature, although it does have some effect in relation to political division. See Sapiezynski P and others, ‘Algorithms That “Don’t See Color”: Comparing Biases in Lookalike and Special Ad Audiences’ (*arXiv*, 2019) <<http://arxiv.org/abs/1912.07579>> accessed 3 August 2022.

³²⁵ Zang J, ‘Solving the Problem of Racially Discriminatory Advertising on Facebook’ (*The Brookings Institution, Artificial Intelligence and Emerging Technology (AIET) Initiative*, 19 October 2021) <<https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/>> accessed 20 June 2022, in reference to: Hanson A and Hawley Z, ‘Where Does Racial Discrimination Occur? An Experimental Analysis across Neighborhood and Housing Unit Characteristics’ (2013) 44 *Regional Science and Urban Economics*; and Bertrand M and Mullainathan S, ‘Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination’ (National Bureau of Economic Research, 2003) w9873 <<http://www.nber.org/papers/w9873.pdf>> accessed 2 August 2022.

³²⁶ Lambrecht A and Tucker C, ‘Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads’ (2019) 65 *Management Science* 2966, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260>.

through market mechanisms, and they highlight the challenges this creates for policies to address the issue. Ali et al. find evidence that discriminatory ad delivery can emerge based on engagement and viewing patterns independently of the targeting stage that the advertiser has the most control over³²⁷. They note that “because different users are valued differently by advertisers, in a setting of limited user attention, [this] leads to a tension between providing a useful service for users and advertisers, fair ad delivery, and the platform’s own revenue goals”³²⁸.

2.2.3 Manipulation

Manipulation can be thought of as imposing a hidden or covert influence on another person’s decision-making, disrupting their capacity for self-authorship of their choices³²⁹.

This section will focus on a variety of categories of potentially manipulative practices linked to digital advertising that have been studied by scholars.

2.2.3.1 Targeting at an individual level

Some digital advertising infrastructures facilitate messages to be targeted to the level of specific individuals. A study by González-Cabañas et al. found that Facebook’s ad infrastructure can uniquely target a user with a 90% probability of success³³⁰. They suggest that a cyber-attacker that has a full list of a user’s interests could uniquely target them using just four of their interests as targeting criteria. The study concludes that the “Facebook Advertising Platform can be systematically exploited to deliver ads exclusively to a specific user”.

The ability to target messages at the level of the individual has raised concerns around the use of these technologies for stalking and manipulation³³¹. Although

³²⁷ Ali M and others, ‘Discrimination through Optimization: How Facebook’s Ad Delivery Can Lead to Biased Outcomes’ (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1, <<https://arxiv.org/abs/1904.02095>>.

³²⁸ Ali M and others, ‘Discrimination through Optimization: How Facebook’s Ad Delivery Can Lead to Biased Outcomes’ (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1, p. 25, <<https://arxiv.org/abs/1904.02095>>.

³²⁹ Susser D, Roessler B and Nissenbaum HF, ‘Online Manipulation: Hidden Influences in a Digital World’ [2018] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3306006>> accessed 2 June 2022.

³³⁰ González-Cabañas J and others, ‘Unique on Facebook: Formulation and Evidence of (Nano)Targeting Individual Users with Non-PII Data’, *Proceedings of the 21st ACM Internet Measurement Conference* (ACM, 2021) <<https://dl.acm.org/doi/10.1145/3487552.3487861>> accessed 2 June 2022.

³³¹ Hirsh J B, Kang S K and Galen V, ‘Personalized Persuasion: Tailoring Persuasive Appeals to Recipients’ (2012) *Personality Traits. Psychological Science* 23, 6 (2012), 578–581 <<https://journals.sagepub.com/doi/abs/10.1177/0956797611436349>>; Matz S C, Kosinski M, Nave G and Stillwell D J, ‘Psychological targeting as an effective approach to digital mass persuasion’ (2017)

these studies provide strong evidence to suggest that advertisers and their agencies are theoretically able to target on an individual level through Facebook, which in turn could be used to manipulate users, there is little available data to indicate how widely this occurs. However, a variety of businesses, anecdotes and online guides claim to further document these practices and even to sell the use of digital advertising tools in this way as a service³³².

2.2.3.2 Vulnerability

A 2017 leaked Meta document described how the firm could analyse when young people feel "stressed", "defeated", "overwhelmed", "anxious", "nervous", "stupid", "silly", "useless" and a "failure"³³³, creating concerns around the potential for these capabilities to generate advertising revenue for the company. Additionally, concerns have been raised about the online gambling industry's ability to use digital advertising techniques to monitor and exploit users with gambling disorders³³⁴. Regulating misuse of types of vulnerability in advertising has long been a priority in the EU, as illustrated by the relevant provisions in the Unfair Commercial Practices Directive (specifically, Recital 18 and Article 5.3).

2.2.3.3 Political "microtargeting"

In political and electoral contexts, concerns have been raised that the ability to target ads at a highly individual and personalised level turns "citizens into objects of manipulation and undermines the public sphere by thwarting public deliberation, aggravating political polarisation, and facilitating the spread of misinformation"^{335, 336}. The highest profile example of this was the Cambridge Analytica scandal, where the firm built and deployed psychographic profiles using

Proceedings of the National Academy of Sciences 114, 48 (2017), 12714–12719, <<https://www.pnas.org/doi/10.1073/pnas.1710966114>>; and Dubois D, Rucker D D and Galinsky A D, 'Dynamics of Communicator and Audience Power: The Persuasiveness of Competence versus Warmth' (2016), *Journal of Consumer Research* 43, 1, 68–85 <<https://www.insead.edu/sites/default/files/assets/faculty-personal-site/david-dubois/documents/Dubois-Rucker-and-Galinsky-JCR-2016.pdf>>.

³³² Faddoul M, Kapuria R and Lin L, 'Sniper Ad Targeting' (10 May 2019) <https://www.ischool.berkeley.edu/sites/default/files/sproject_attachments/sniper_ad_targeting_final_report.pdf>.

³³³ Davidson D, 'Facebook Targets 'Insecure' to Sell Ads.' (*The Australian*, 2017), <<https://www.proquest.com/docview/1893187270/10BFB8730256498APQ/1?accountid=14511>>.

³³⁴ Christl W, 'Digital Profiling in the Online Gambling Industry' (*Cracked Labs*, January 2022) <<https://crackedlabs.org/en/gambling-data>> and Zarb-Cousin M, 'Clean Up Gambling Submits Evidence to ICO on Data Abuse' (*Clean Up Gambling*, 16 August 2022) <<https://cleanupgambling.com/news/clean-up-gambling-submits-evidence-to-ico-on-data-abuse>> accessed 6 October 2022.

³³⁵ Barocas S, 'The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process', *Proceedings of the first edition workshop on Politics, elections and data - PLEAD '12* (ACM Press 2012) <<http://dl.acm.org/citation.cfm?doid=2389661.2389671>> accessed 6 June 2022;

³³⁶ Gorton WA, 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy' (2016) 38 *New Political Science* 61.

information gathered from Facebook profiles with the aim of influencing voters' electoral choices and turnout probability. This led to action by both data protection authorities and electoral management bodies. Large scale political microtargeting campaigns that facilitated the spread of misinformation have also been reported around the world, including in the US, the Philippines and Russia³³⁷. To tackle some of these issues, the European Commission has proposed a regulation on transparency and targeting of political advertising³³⁸.

The data practices of political parties, some of which accumulate and enrich large amounts of data about the electorate³³⁹, have led regulators and academics to express concern about illegal data processing by political actors³⁴⁰, reiterating earlier calls on the topic from global data protection authorities³⁴¹.

Concerns have also been raised about the potential for microtargeting to be used as a form of interference by foreign actors. This was first brought to mainstream attention through Russian-backed Internet Research Agency (IRA) efforts using Facebook and other platforms, which included advertising. In 2017, Meta admitted that 3,000 ads placed by 470 Facebook registered accounts or pages were purchased by Russian state-affiliated groups in the 2016 US elections³⁴². Riley suggests that the sheer scale of major platforms creates a considerable security risk, describing Facebook's operations as providing "a single 'attack surface' of 2.8 billion users" who can be identified at "a very granular level"³⁴³. When combined with Facebook's engagement-oriented algorithm, he highlights the potential for major platforms to act as a vehicle for authoritarian governments to "reach deep"

³³⁷ Coppins M, 'The Billion-Dollar Disinformation Campaign to Re-elect the President' (*The Atlantic*, 10 February 2020) <<https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/>> accessed 2 June 2022.

³³⁸ Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising. COM(2021) 731 Final.

³³⁹ Brown I, Marsden C T, Lee J & Veale, M, 'Cybersecurity for Elections: A Commonwealth Guide on Best Practice' (*Commonwealth*, 2020) <<http://sro.sussex.ac.uk/id/eprint/91952/>> accessed 12 April 2022.

³⁴⁰ Blasi Casagran C and Vermeulen M, 'Reflections on the Murky Legal Practices of Political Micro-Targeting from a GDPR Perspective' (2021) 11 *International Data Privacy Law* 348; European Data Protection Supervisor, *EDPS Opinion on online manipulation and personal data (Opinion 3/2018)*, <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf>; 'Audits of data protection compliance by UK political parties' (Information Commissioner's Office, November 2020) <<https://ico.org.uk/media/action-weve-taken/2618567/audits-of-data-protection-compliance-by-uk-political-parties-summary-report.pdf>>.

³⁴¹ ICDPPC. *Resolution on the Use of Data for Political Communication*. 27th International Conference of Data Protection and Privacy Commissioners, Montreux, Switzerland. (2005, September 14-16) <https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_en.pdf>.

³⁴² Kim YM and others, 'The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook' (2018) 35 *Political Communication* 515, p. 516.

³⁴³ Riley A, 'Can Brussels Take Security Seriously? Can the EU Move Beyond Its "Common Market" DNA?' (*The European Journal - New Direction*) <<https://newdirection.online/the-european-journal/article/can-brussels-take-security-seriously>> accessed 18 July 2022.

into democracies. In facilitating the identification and targeting of provocative high-engagement content to users in specific communities or localities with great accuracy, Riley concludes that major platforms may therefore have offered foreign state actors a greater capacity to sow hatred between groups³⁴⁴.

Kim et al. traced the sponsors and sources behind the issue campaigns of five million Facebook ads in the context of the 2016 US elections, finding that the majority did not report (as would be expected) to the US Federal Electoral Commission (FEC) and were placed by “anonymous” groups whose true identity is little known to the public. Just under half of the groups placing ads were classified as “suspicious”, with one in five later being identified as Russian-affiliated foreign interference by the US House of Representatives Intelligence Committee³⁴⁵. In general, however, given the covert nature of foreign interference and patchy available data, measuring foreign interference using digital advertising tools remains difficult today³⁴⁶. Additionally, while studies suggest that political microtargeting is used to influence voters, some researchers question whether hyper-targeted political advertising is effective at persuading voters to begin with³⁴⁷. One study suggests that “voters seem to prefer being solicited based on broad principles and collective benefits”, and that “narrower appeals come with risks, since they lead to diminished support among non-group members who may easily be mistargeted”³⁴⁸.

³⁴⁴ Riley A, ‘Can Brussels Take Security Seriously? Can the EU Move Beyond Its “Common Market” DNA?’ (*The European Journal - New Direction*) <<https://newdirection.online/the-european-journal/article/can-brussels-take-security-seriously>> accessed 18 July 2022.

³⁴⁵ Kim YM and others, ‘The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook’ (2018) 35 *Political Communication* 515.

³⁴⁶ Leerssen P and others, ‘Platform Ad Archives: Promises and Pitfalls’ (2019) 8 *Internet Policy Review* <<https://policyreview.info/node/1421>> accessed 10 May 2022; Leerssen P and others, ‘News from the Ad Archive: How Journalists Use the Facebook Ad Library to Hold Online Advertising Accountable’ [2021] *Information, Communication & Society* 1.

³⁴⁷ Kraus R, ‘How Well Does “microtargeted Psychographic Advertising” Work Anyway?’ (*Mashable*, 24 March 2018) <<https://mashable.com/article/how-microtargeted-ads-affect-behavior>> accessed 20 June 2022; Kalla JL and Broockman De, ‘The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments’ (2018) 112 *American Political Science Review* 148, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042867#>.

³⁴⁸ Hersh ED and Schaffner BF, ‘Targeted Campaign Appeals and the Value of Ambiguity’ (2013) 75 *The Journal of Politics* 520, <<https://www.journals.uchicago.edu/doi/abs/10.1017/s0022381613000182>>.

2.3 What is the environmental impact of the way that digital advertising has evolved?

The data processing required for digital advertising leads to high energy consumption and emissions. This is linked to the collection of large amounts of personal data to profile individuals for digital advertising purposes, and the energy consumption involved in delivering digital advertising. Between 8-15% of the page loading activities of the top 350 news websites are linked to advertising-related content. A significant amount of this data processing is likely to be linked to fraudulent activity that doesn't generate any value for

2.3.1 Energy cost of end-user devices

Growing attention is being drawn to the environmental effects of information and communications technologies (ICTs), and advertising technologies are no different. By one estimate, the share of total global greenhouse gas (GHG) emissions coming from ICTs could be as high as 2.1-3.9%³⁴⁹. Despite some evidence suggesting that ICT is becoming more efficient, studies indicate that ICT emissions are increasing, and will continue to do so in the absence of targeted intervention, in part owing to factors including increasing investment in blockchain, the Internet of Things (IoT) and artificial intelligence (AI)³⁵⁰. Evaluating the share of emissions caused specifically by digital advertising is challenging, owing in part to the opacity of the ecosystem and collateral effects on consumer behaviour. One study suggests that digital advertising in 2016 consumed 20-282TWh of energy, producing approximately 60Mt of CO₂e emissions³⁵¹, which has likely grown in line with the expansion of digital advertising in subsequent years. On a more granular level, one company has estimated that "one gram of carbon is produced every time an ad impression is generated"³⁵².

³⁴⁹ Freitag C and others, 'The Climate Impact of ICT: A Review of Estimates, Trends and Regulations' (*arXiv*, 3 February 2021) <<http://arxiv.org/abs/2102.02622>> accessed 21 June 2022.

³⁵⁰ Freitag C and others, 'The Climate Impact of ICT: A Review of Estimates, Trends and Regulations' (*arXiv*, 3 February 2021) <<http://arxiv.org/abs/2102.02622>> accessed 21 June 2022.

³⁵¹ Pärssinen M and others, 'Environmental Impact Assessment of Online Advertising' (2018) 73 *Environmental Impact Assessment Review* 177.

³⁵² This figure is based on modelling by Scope3, which considers a combination of base emissions, supply path emissions, and creative emissions. Under the model, base emissions include emissions stemming from publisher content creation and end-user devices (i.e. the emissions created through webpage loading). Supply path emissions are emissions resulting from the various parties involved in targeting and serving an impression (i.e. in the interactions between vendors). Creative emissions refer to those associated with "creative delivery", for instance the CPU costs of loading the images or videos constituting an advert on a webpage. See: 'Measuring the Carbon Footprint of Programmatic Advertising - Version 1.2' (Scope3, July 2022) and Shields R, 'Brian O'Kelley: "Our Model Is to Get Buyers to Make Emissions Part of

Digital advertising requires computational resources to be used on individuals' devices, the servers employed by the publishers, and the servers employed by various intermediaries which sit between publishers, users and advertisers³⁵³. The use of these resources brings material and energy costs of transmitting data (communication or network costs) and costs of processing data (compute costs).

The computational cost of advertising on users' devices is significant. One study found that approximately 15% of browser page loading activities (network cost) of the 350 top news websites relate to advertising-related content, although this is 7% lower on mobile websites as "mobile pages include fewer and well-optimised ads"³⁵⁴. Of these websites, 20% spend more than 30% of the computing time it takes to load the website itself on loading ads³⁵⁵. The same study found that domains owned and run by Alphabet are responsible for the highest contribution to the computation of ads on the web, together accounting for approximately 35% of computational resources³⁵⁶. They are also responsible for the highest network cost of digital advertising, together accounting for approximately 51% of total ad network cost³⁵⁷.

On mobile, many apps have embedded software libraries for advertising and tracking that can consume a large proportion of the device's total energy. For example, one study reports that the game Angry Birds, which is popular throughout Europe, consumed 65-75% of the energy it used for advertising purposes (including user tracking and displaying advertising) compared to only 25-35% of energy for actual gameplay³⁵⁸. Another study notes that free apps on the Windows Phone platform consume on average 23% of an app's total energy

Their Spending Decisions" (*Digiday*, 15 March 2022) <<https://digiday.com/media/brian-okelley-our-model-is-to-get-buyers-to-make-emissions-part-of-their-spending-decisions/>> accessed 21 September 2022.

³⁵³ 'Appendix M: intermediation in open display advertising' in 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p. M5, <[https://assets.publishing.service.gov.uk/media/5fe495c28fa8f56afaf406d4/Appendix M - intermediation in open display advertising WEB.pdf](https://assets.publishing.service.gov.uk/media/5fe495c28fa8f56afaf406d4/Appendix_M_-_intermediation_in_open_display_advertising_WEB.pdf)>.

³⁵⁴ Pourghassemi B and others, 'AdPerf: Characterizing the Performance of Third-Party Ads' (2021) 5 Proceedings of the ACM on Measurement and Analysis of Computing Systems 1, p. 3.

³⁵⁵ Pourghassemi B and others, 'AdPerf: Characterizing the Performance of Third-Party Ads' (2021) 5 Proceedings of the ACM on Measurement and Analysis of Computing Systems 1, p. 13.

³⁵⁶ Pourghassemi B and others, 'AdPerf: Characterizing the Performance of Third-Party Ads' (2021) 5 Proceedings of the ACM on Measurement and Analysis of Computing Systems 1, p. 17.

³⁵⁷ Pourghassemi B and others, 'AdPerf: Characterizing the Performance of Third-Party Ads' (2021) 5 Proceedings of the ACM on Measurement and Analysis of Computing Systems 1, p. 18.

³⁵⁸ Pathak A, Hu YC and Zhang M, 'Where Is the Energy Spent inside My App?: Fine Grained Energy Accounting on Smartphones with Eprof', *Proceedings of the 7th ACM 90 European conference on Computer Systems - EuroSys '12* (ACM Press, 2012), p. 39 <<http://dl.acm.org/citation.cfm?doid=2168836.2168841>> accessed 10 May 2022.

through advertising-related communication costs³⁵⁹, although given the study's age and reference to an operating system with a small market share, it is unclear how reflective this is of Android or iOS's energy consumption. Papadopoulos et al. estimate that 9% of mobile battery life is consumed by the network costs of advertising and analytics-related traffic³⁶⁰. Other authors emphasise that this is exacerbated by poor protocol design (such as leaving connections open) and communicating with many third parties, noting that some advertising libraries can more than double the power consumption of a device displaying and refreshing advertising banners³⁶¹.

Pourghassemi et al. point out that these costs have grown over time due to the growing complexity of digital advertising, and align with the emergence of techniques and advertising models which involve large amounts of data processing and sharing among different third parties³⁶².

2.3.2 Environmental impact of waste and fraud

Digital advertising is known to involve a significant number of fraudulent clicks, views and other activity by "non-users". Such fraud can be achieved through a variety of techniques. Conventional ad fraud sees a limited number of servers generating a large amount of traffic, typically claiming to represent a large proportion of real individual users. To avoid detection, researchers have highlighted a move towards "crowd fraud"³⁶³ where fraud attacks originate from many sources, but with a low amount of traffic coming from each source³⁶⁴. Physical "click-farms", designed to manipulate websites and apps for profit, are being increasingly identified; often they are racks of mobile devices controlled by

³⁵⁹ Mohan P, Nath S & Riva O, 'Prefetching mobile ads: Can advertising systems afford it?' (2013) *Proceedings of the 8th ACM European Conference on Computer Systems*, 267–280.

³⁶⁰ Papadopoulos P, Kourtellis N and Markatos EP, 'The Cost of Digital Advertisement: Comparing User and Advertiser Views', *Proceedings of the 2018 World Wide Web Conference on World Wide Web – WWW '18* (ACM Press, 2018) <<http://dl.acm.org/citation.cfm?doid=3178876.3186060>> accessed 16 May 2022.

³⁶¹ Vallina-Rodriguez N and others, 'Breaking for Commercials: Characterizing Mobile Advertising', *Proceedings of the 2012 ACM conference on Internet measurement conference – IMC '12* (ACM Press, 2012), p. 352 <<http://dl.acm.org/citation.cfm?doid=2398776.2398812>> accessed 16 May 2022.

³⁶² Pourghassemi B and others, 'AdPerf: Characterizing the Performance of Third-Party Ads' (2021) 5 *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 1, p. 23.

³⁶³ Pooranian Z and others, 'Online Advertising Security: Issues, Taxonomy, and Future Directions' (2021) 23 *IEEE Communications Surveys & Tutorials* 2494; Tian T and others, 'Crowd Fraud Detection in Internet Advertising', *Proceedings of the 24th International Conference on World Wide Web* (International World Wide Web Conferences Steering Committee, 2015) <<https://dl.acm.org/doi/10.1145/2736277.2741136>> accessed 25 May 2022.

³⁶⁴ Tian T and others, 'Crowd Fraud Detection in Internet Advertising', *Proceedings of the 24th International Conference on World Wide Web* (International World Wide Web Conferences Steering Committee, 2015), p. 1100 <<https://dl.acm.org/doi/10.1145/2736277.2741136>> accessed 24 May 2022.

a mix of people and machines³⁶⁵. The characteristics of crowd fraud mean it may produce significantly higher environmental impact than conventional ad fraud, as its structure incentivises the accumulation of physical devices without users³⁶⁶.

The scale of this impact is hard to estimate. Reports on ad fraud tend to originate from digital advertising intermediaries selling ad fraud prevention solutions, who themselves often warn that a huge percentage of clicks or user profiles that can be purchased for targeting online are fraudulent. Ad fraud exposure estimates compiled by research firm BotLab and the World Federation of Advertisers range between 2% and 90%, an uncertainty further underlined by a study indicating that 36% of surveyed advertisers do not know their exposure to fraudulent activity³⁶⁷. One estimate suggests that fraudulent ad traffic was responsible for producing 13.87Mt of CO₂e in 2016, accounting for approximately 23.1% of emissions resulting from the digital advertising ecosystem³⁶⁸. However, the aforementioned uncertainty regarding the share of exposure to ad fraud is a considerable limitation to calculating an accurate figure. Academic commentators have estimated the scale of this problem to be “enormous” and contributing to a sector that can be understood as “subprime” in the same way as the US mortgage market³⁶⁹. Further research is required to accurately assess the environmental impact of ad fraud.

Commentators have also pointed to the environmental costs of advertising on websites and content which have “no value to society”³⁷⁰. A recent report by media consultancy Ebiquity estimated that 10% of programmatic display and video ad spend in the US was being wasted on “made for advertising” clickbait websites which provide little value to advertisers and siphon advertising revenue away from high-quality publishers that invest in journalism³⁷¹. Several industry case studies

³⁶⁵ Ashcraft B, ‘Inside Chinese “Click Farms”’ (*Kotaku*, 18 May 2017) <<https://www.kotaku.com.au/2017/05/inside-chinese-click-farms/>> accessed 25 May 2022; Matsakis L, ‘Look at This Massive Click Fraud Farm That Was Just Busted In Thailand’ (*Vice*, 12 June 2017) <<https://www.vice.com/en/article/43yqdd/look-at-this-massive-click-fraud-farm-that-was-just-busted-in-thailand>> accessed 24 May 2022.

³⁶⁶ Clément L-PP-VP, Jacquemotte QES and Hilty LM, ‘Sources of Variation in Life Cycle Assessments of Smartphones and Tablet Computers’ (2020) 84 *Environmental Impact Assessment Review* 106416.

³⁶⁷ Kotila M, Rumin, R C, & Dhar S, *Compendium of ad fraud knowledge for media investors*. (World Federation of Advertisers and Botlab, 2016), p. 3 <<https://swa-asa.ch/wAssets/docs/publikationen/de/branchenempfehlungen-swa/WFACompendiumofAdFraudKnowledge.pdf>>.

³⁶⁸ Pärssinen M and others, ‘Environmental Impact Assessment of Online Advertising’ (2018) 73 *Environmental Impact Assessment Review* 177.

³⁶⁹ Hwang T, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. (Farrar, Straus and Giroux, 2020).

³⁷⁰ Barwick R, ‘Advertisers Spent \$115 Million on Clickbait Sites, Report Finds’ (*Marketing Brew*, 18 July 2022) <<https://www.marketingbrew.com/stories/2022/07/18/advertisers-spent-usd115-million-on-clickbait-sites-report-finds>> accessed 19 July 2022.

³⁷¹ ‘Tackling Responsible Media’ (*Ebiquity*, 19 July 2022) <<https://www.ebiquity.com/news-insights/viewpoints/tackling-responsible-media/>> accessed 19 July 2022.

support the notion that significant amounts of digital advertising spend result in wasted impressions, leading to unnecessary data processing and carbon emissions. In 2017, JP Morgan Chase reduced the number of websites they were advertising on from 400,000 to 5,000 after discovering that ads on only 3% of websites led to activity beyond an impression³⁷². In an interview with The New York Times, JP Morgan Chase's Chief Marketing Officer said that "we haven't seen any deterioration on our performance metrics" as a result of the change.³⁷³ Similarly, Procter & Gamble reported that cutting \$100 million in "largely ineffective" digital ads didn't lead to any reduction in growth rates³⁷⁴. In 2020 Airbnb's CEO indicated that when the company cut more than \$500 million in digital advertising spend during the pandemic, they "still had 95% of the same traffic as the year before"³⁷⁵. When Uber turned off two-thirds of digital ad spend, they reported "no change" in the number of app installs³⁷⁶, leading to them filing and winning a lawsuit against intermediary Phunware for ad fraud³⁷⁷.

Several advertisers have also pointed to waste generated by buying advertising that cannibalises organic (unpaid) placements, particularly in search and on retail sites. In 2022, Simple Modern reported cutting \$10 million in Amazon ads because they discovered that the people clicking on their ads were already planning to purchase their products³⁷⁸. A similar realisation was had by eBay more than nine years ago when they conducted a study that indicated they were only getting \$0.25 of value for every \$1 they spent on Google paid search because "existing

³⁷² Maheshwari S, 'Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results.' (*New York Times*, 30 March 2017) <<https://www.nytimes.com/2017/03/29/business/chase-ads-youtube-fake-news-offensive-videos.html>> accessed 2 October 2022.

³⁷³ Maheshwari S, 'Chase Had Ads on 400,000 Sites. Then on Just 5,000. Same Results.' (*New York Times*, 30 March 2017) <<https://www.nytimes.com/2017/03/29/business/chase-ads-youtube-fake-news-offensive-videos.html>> accessed 2 October 2022.

³⁷⁴ Terlep S and Bruell A, 'P&G Cuts More Than \$100 Million in "Largely Ineffective" Digital Ads' (*Wall Street Journal*, 27 July 2017) <<https://www.wsj.com/articles/p-g-cuts-more-than-100-million-in-largely-ineffective-digital-ads-1501191104>> accessed 19 July 2022.

³⁷⁵ Spanier G, 'Airbnb Slashes Spend in Permanent Shift from Performance Marketing to Brand' (*Airbnb*, 1 March 2021) <https://www.campaignlive.co.uk/article/airbnb-slashes-spend-permanent-shift-performance-marketing-brand/1708621?utm_source=website&utm_medium=social> accessed 19 July 2022.

³⁷⁶ Samarajiva I, 'How Uber Discovered That 80% of Its Ads Were Useless' (*Medium*, 19 February 2020) <<https://indica.medium.com/how-uber-discovered-that-80-of-its-ads-were-useless-bb4d96ee46c8>> accessed 19 July 2022.

³⁷⁷ 'Reed Smith Wins Multi-Million Dollar Advertising Fraud Suit for Uber' (*Reed Smith LLP*) <<https://www.reedsmith.com/en/news/2021/01/reed-smith-wins-multimillion-dollar-advertising-fraud-suit-for-uber>> accessed 19 July 2022.

³⁷⁸ Porter B, 'A Thread about Our Change of Heart with Amazon Advertising': <<https://twitter.com/jbryanporter/status/1507500277175361538>> accessed 19 July 2022 cited by Augustine Fou in Fou A, 'A Positive Story About Digital Marketing -- They Stopped Spending' (*LinkedIn*, 27 March 2022) <<https://www.linkedin.com/pulse/positive-story-digital-marketing-stopped-spending>> accessed 19 July 2022.

customers would have come to eBay regardless³⁷⁹. All of this advertising entails extensive data processing which, according to these studies, may be generating unnecessary carbon emissions and generating very little (or no) value to advertisers.

2.3.3 Industry responses to the environmental impact of digital advertising

Several companies, including advertisers and intermediaries, have looked to mitigate the environmental impact of their digital advertising activities, some through pledging to offset the carbon costs of their servers by funding climate projects³⁸⁰, others through conducting research into their own emissions³⁸¹. A potential obstacle to a company reducing its emissions in relation to advertising is likely to be the opacity of the supply chain, which could make it difficult to assess the level and sources of energy consumption. As such, companies are developing tools to help quantify their emissions with the aim of understanding what the most effective responses might be. Scope3, which describes itself as a “public benefit corporation”³⁸², uses a combination of operational data and publicly available data to model “the core inputs and outputs for each product and service in the [digital advertising] supply chain”³⁸³ in order to enable companies throughout the digital advertising ecosystem to calculate their emissions. This type of technology could potentially facilitate the identification of measures to limit digital advertising practices that have a detrimental environmental impact, as well as areas where efficiency could be improved. In 2022, Scope3’s technology was used by The Trade Desk, which owns one of the industry’s largest demand-side platforms (DSPs), to calculate the impact on emissions of their decision to stop redundant traffic being sent to Google’s Open Bidding³⁸⁴. The project estimated that reducing waste in this way may have eliminated 5,387 tons of CO₂ per year in the US alone³⁸⁵. However, this approach may require a higher level of transparency than currently

³⁷⁹ Fisman R, ‘Did eBay Just Prove That Paid Search Ads Don’t Work?’ (*Harvard Business Review*, 2013) <<https://hbr.org/2013/03/did-ebay-just-prove-that-paid>> accessed 2 October 2022.

³⁸⁰ ‘Good-Loop’ (*Ecologi*) <<https://ecologi.com/good-loop>> accessed 19 July 2022; ‘Good-Loop: Our Story’ (*Good-Loop*, 7 July 2022) <<https://good-loop.com/our-story>> accessed 19 July 2022.

³⁸¹ Graham M, ‘Digital Advertising Companies Look to Reduce the Industry’s Carbon Footprint’ (*Wall Street Journal*, 2022) <<https://www.wsj.com/articles/digital-advertising-reduce-carbon-footprint-11655495160>> accessed 27 June 2022.

³⁸² ‘Introducing Scope3: The Source of Truth for Supply Chain Emissions Data’ (*Scope3*) <<https://www.scope3.com/news/introducing-scope3>> accessed 18 July 2022.

³⁸³ ‘Scope3’ <<https://www.scope3.com/old-home>> accessed 18 July 2022.

³⁸⁴ The impact of The Trade Desk’s move away from Open Bidding calculated as 5,387 tons of CO₂ per year in the US. O’Kelley B, ‘How TTD Saved 5,387 Tons of CO₂ - and You Can Too’ (*BOKonAds*, 20 April 2022) <<https://bokonads.com/how-ttd-saved-5387-tons-of-co2/>> accessed 27 June 2022.

³⁸⁵ O’Kelley B, ‘How TTD Saved 5,387 Tons of CO₂ - and You Can Too’ (*BOKonAds*, 20 April 2022) <<https://bokonads.com/how-ttd-saved-5387-tons-of-co2/>> accessed 27 June 2022.

exists in the digital advertising ecosystem. As Scope3 have pointed out, “[to measure, manage and ultimately reduce their carbon footprint] brands must demand visibility, data and strategies to help them factor emissions into every campaign decision they make. Soon, brand marketers will not only require their agencies and ad-tech providers to provide campaign success metrics, but also insights into what steps were taken to run effective campaigns while using the least amount of energy”³⁸⁶.

While there have likewise been efforts from industry bodies to reduce emissions, for instance the UK Advertising Association’s Ad Net Zero initiative, a limitation of many initiatives is their lack of specific focus on digital advertising, despite its significant impact relative to other sources of emissions. The Ad Net Zero report, for example, sets out a five-step action plan which refers to emissions from travel, the production of adverts, industry events and office energy consumption, but only briefly mentions digital ad emissions in the context of media planning and buying, including the digital carbon impact tool, DIMPACT³⁸⁷. IAB Europe, however, has recently launched a new initiative designed to develop “practical and measurable steps that participants can implement to decarbonise their digital media” through a “Green Media standard”. Although this initiative is still in the very early stages, it appears to aim to tackle environmental issues related to digital advertising directly.

Mikko Kotila, CTO of the ad company Cavai and researcher in the fields of advertising and data science, notes that at such an early stage in the development of most industry initiatives, “it will be hard to separate meaningful efforts from publicity ploys”³⁸⁸. It could be argued that approaching the problem in a piecemeal manner through offsetting emissions or making donations to climate initiatives ignores some of the more systemic issues related to the advertising ecosystem, such as complexity and lack of transparency, that are heavy contributors to the inefficiencies driving energy consumption.

Some intermediaries have been incentivised to switch to Google’s cloud infrastructure as part of their efforts to reduce emissions, based on Google’s claims that it matches its global electricity use with wind and solar energy purchases, only uses carbon-based power at certain times and locations across its data

³⁸⁶ ‘Advertising: A Missing Link in Successful Corporate Climate Actions Plans’ (*Scope3*) <<https://www.scope3.com/news/advertising-a-missing-link-in-successful-corporate-climate-action-plans>>

³⁸⁷ DIMPACT is a project aiming to simplify the measurement of carbon emissions in digital media. ‘Advertising’s Response to the Climate Emergency’ (*Ad Net Zero*) <<https://adnetzero.com/>> accessed 19 July 2022; ‘About DIMPACT’ (*DIMPACT*) <<https://dimpact.org/about>> accessed 19 July 2022.

³⁸⁸ Graham M, ‘Digital Advertising Companies Look to Reduce the Industry’s Carbon Footprint’ (*Wall Street Journal*, 2022) <<https://www.wsj.com/articles/digital-advertising-reduce-carbon-footprint-11655495160>> accessed 27 June 2022.

centres and its pledge to “match its operational electricity use with nearby carbon-free energy” every hour of the day³⁸⁹. For example, in 2019 ad exchange OpenX announced it would be migrating its entire infrastructure to Google Cloud, claiming this would allow it to achieve sufficient reductions in emissions to receive a “carbon neutral” certification. Google claims that this move reduced overall latency, “especially when sending requests to Google Marketing Platform products such as Display and Video 360” while OpenX’s Chief Architect said that “Google is one of our biggest exchange bidding partners, so keeping that ad traffic within the Google network just makes sense”. It is important to note, however, the recent competition concerns raised in relation to interoperability and self-preferencing between Google services, as highlighted in the 2021 decision of the French competition authority, *Autorité de la Concurrence* (ADLC), and an ongoing investigation by the UK competition authority, the Competition and Markets Authority (CMA)³⁹⁰.

2.4 How do the efficacy and efficiency benefits of the evolution of digital advertising compare to the societal and environmental impact?

The most widely used products in digital advertising rely on large amounts of personal data and profiling of individuals. However, there is limited evidence to suggest that the efficiency and efficacy gains to advertisers and publishers outweigh the societal impact of these products. There is a lack of independent analysis to assess the benefits of using personal data and profiling in advertising. The few studies that do exist fail to take into account important considerations such as the impact of fraud and buyer expectations.

³⁸⁹ ‘Operating on 24/7 Carbon-Free Energy by 2030’ (*Google Sustainability*) <<https://sustainability.google/progress/energy/>> accessed 19 July 2022.

³⁹⁰ ‘Decision 21-D-11 of June 07, 2021 Regarding Practices Implemented in the Online Advertising Sector’ (*Autorité de la concurrence*, 26 July 2021) <<https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-online-advertising-sector>>; ‘Google Probed over Potential Abuse of Dominance in Ad Tech’ (*GOV.UK*) <<https://www.gov.uk/government/news/google-probed-over-potential-abuse-of-dominance-in-ad-tech>> accessed 19 July 2022.

2.4.1 Studies of the efficacy and efficiency benefits of digital advertising

In this section, we consider the question of the efficacy and efficiency benefits of digital advertising, primarily with reference to its outcomes for publishers, due to the importance of advertising in funding online services.

A genre of studies carried out by academics, industry and regulators considers the impact on the cost or revenue generated by an ad in the presence or absence of cookie data, which enables more advanced profiling, targeting and measurement. A range of studies show short-term decreases to publishers for bids that do not have cookies available within the current set-up of advertising exchanges³⁹¹. A Google study³⁹² replicated and expanded by the CMA³⁹³ found that blocking third-party cookies decreases the short-run revenue to publishers by 70%. Conversely, Marotta et al. have estimated this number could be as low as a 4% decrease for publishers³⁹⁴.

The large discrepancies between these two studies could be attributed to a number of factors. The CMA identified several factors which could have affected Google's estimation of the impact of turning off cookies on publisher revenues³⁹⁵. For example, the CMA was unable to statistically mitigate against the fact that Google's sample included a disproportionate number of impressions served by non-Google supply-side platforms (SSPs), which they note could have led to an overestimation of the impact of turning off third-party cookies. The CMA furthermore notes that the analysis excludes impressions served to users logged in to Google's services, which typically represent 20-30% of impressions. As a result, the CMA concludes that "the sample is not representative of traffic through

³⁹¹ Johnson GA, Shriver SK and Du S, 'Consumer Privacy Choice in Online Advertising: Who Opt's Out and at What Cost to Industry?' (2020) 39 Marketing Science 33; Ravichandran D and Korula N, 'Effect of Disabling Third-Party Cookies on Publisher Revenue' (27 August 2019)

<https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf>.

³⁹² Ravichandran D and Korula N, 'Effect of Disabling Third-Party Cookies on Publisher Revenue' (27 August 2019) <https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf>.

³⁹³ 'Appendix F: the role of data in digital advertising' in 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p. F30-31, <https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf>.

³⁹⁴ Marotta V, Abhishek V and Acquisti A, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (2019) <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>.

³⁹⁵ 'Appendix F: the role of data in digital advertising' in 'Online Platforms and Digital Advertising - Market Study Final Report' (Competition and Markets Authority, 2020), p. F30-31 and F39-65 <https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf>.

the Google stack from UK users³⁹⁶. The Marotta et al. study similarly has limitations which make it difficult to assess its representativeness. Most importantly, Marotta et al. consider impressions served on a selection of websites owned by a single publisher. Although the nature of these websites varies (covering news, lifestyle, fashion and automobile, among others), the researchers acknowledge that “they may not generalise to the entire universe of existing websites”³⁹⁷. Furthermore, the Marotta et al. study does not take into account the cost of fraud and arbitrage on publisher revenues, and it is not clear whether the Google analysis did either. This may have led to an overestimation of the impact of turning off third-party cookies in both cases. There are also significant regional differences in the samples studied. Google’s sample only includes impressions served in the UK, while the Marotta et al. sample includes impressions served in the US (72%), Europe (15%) and Oceania (4.3%).

It is particularly important to note that these studies are often undertaken in the context of a market acclimatised to bid requests that contain third-party cookie data. It is therefore unsurprising that bids going against the current mainstream approach to targeting have substantially smaller desirability for advertisers. As the CMA points out as a caveat to its analysis of Google’s data, “omitting cookie IDs from bid requests might generate adverse selection issues, where advertisers interpret the lack of cookie information as a signal of poor quality – especially from browsers that do not have tracking prevention enabled by default”³⁹⁸. This is coupled with a lack of comparison with alternative models, such as detailed contextual modelling of the website being visited, or the use of local targeting through privacy-enhancing technologies. Empirical studies already indicate the value of contextual data (e.g. full URLs) in advertising markets but tend to focus on its complementarity in relation to brand reputation alongside high-quality or niche websites³⁹⁹. In the short run, it is therefore unsurprising that the market response to a bid request without cookie data is priced down compared to those with cookie data, as limited incentives exist to appraise alternative signals for how much to pay for an impression. Some advertisers simply choose not to bid at all

³⁹⁶ ‘Appendix F: the role of data in digital advertising’ in ‘Online Platforms and Digital Advertising - Market Study Final Report’ (Competition and Markets Authority, 2020), p. F41.

<https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_role_of_data_in_digital_advertising_v.4_WEB.pdf>.

³⁹⁷ Marotta V, Abhishek V and Acquisti A, ‘Online Tracking and Publishers’ Revenues: An Empirical Analysis’ (2019), p. 29 <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>.

³⁹⁸ ‘Appendix F: the role of data in digital advertising’ in ‘Online Platforms and Digital Advertising - Market Study Final Report’ (Competition and Markets Authority, 2020), p. F64

<https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_role_of_data_in_digital_advertising_v.4_WEB.pdf>.

³⁹⁹ Ada S, Abou Nabout N and Feit EM, ‘Context Information Can Increase Revenue in Online Display Advertising Auctions: Evidence from a Policy Change’ [2022] *Journal of Marketing Research*, 002224372110702, <<https://doi.org/10.1177/00222437211070219>>.

on platforms such as Safari which block cookies, according to a quantitative study from a fingerprinting vendor⁴⁰⁰. This is supported by some of the interviews carried out for this study. In addition, there is a lack of studies estimating the economic impact of the reduction of tracking when such capacities are reduced for all actors simultaneously. That means that the long-term effects are ultimately difficult to measure. Indeed, the CMA notes that “the analysis [of Google’s data] is unable to answer the question of what the long-run, market-wide effects of the removal of third-party cookies throughout the entire ecosystem would be [...] because advertisers, platforms and publishers would be expected to respond to this change in ways that are difficult to predict”⁴⁰¹.

Also, these studies tend only to focus on what this study defines as “other” display advertising, delivered programmatically and served on publisher sites and apps. There is limited data available to assess and compare different types of targeting and, most importantly, different approaches to using personal data in relation to advertising bought directly from large platforms, even though these channels make up a significant part of the digital advertising market, as discussed in section 1. The interviews conducted for this study support this. As outlined in section 4.3, advertisers say they feel they do not have enough data to assess the efficacy or efficiency of their ads when working with large platforms, despite many of them spending a significant proportion of their advertising budgets on services provided by these companies.

In summary, the few available studies on the revenues that publishers can generate from digital advertising based on personal data and profiling vary significantly in their findings. Additionally, it is difficult to draw comparisons between the current digital advertising model and one that would rely on less personal data using actual market data. That’s because the market is accustomed to the current model, which could lead to alternatives being undervalued in auctions, at least in the short-term. That means that publishers that try to sell their inventory without offering targeting based on profiling may find it more difficult to find higher bids. This highlights the role that network effects and advertisers’ perceptions of the effectiveness of digital advertising can have on publishers’ revenues.

⁴⁰⁰ ‘Cookie Rejection Report 2020’ (Flashtalking, 2020), p. 5, <<https://static1.squarespace.com/static/5c17fee58ab722e19b765b9d/t/5ebb2cad66d47b4c5c9f21a9/1589324990858/Flashtalking+Cookie+Rejection+Report+2020.pdf>>.

⁴⁰¹ ‘Appendix F: the role of data in digital advertising’ in ‘Online Platforms and Digital Advertising - Market Study Final Report’ (Competition and Markets Authority, 2020), p. F30-31, <https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf>.

2.4.2 Efficiency and intermediation

Advertisers and publishers find themselves at either end of a complex chain of intermediation, which often lacks transparent workings. Regulators, government agencies and industry groups have warned of hidden fees or an “ad tech tax” whereby a large and difficult-to-measure portion of advertisers’ spend is lost to intermediaries before reaching publishers. In 2017 the Chief Brand Officer of the world’s largest advertiser, Procter & Gamble, described the digital advertising supply chain as “murky at best, and fraudulent at worst”, complaining that “we serve ads to consumers through a non-transparent media supply chain with spotty compliance to common standards, unreliable measurement, hidden rebates and new inventions like bot and methbot fraud”⁴⁰².

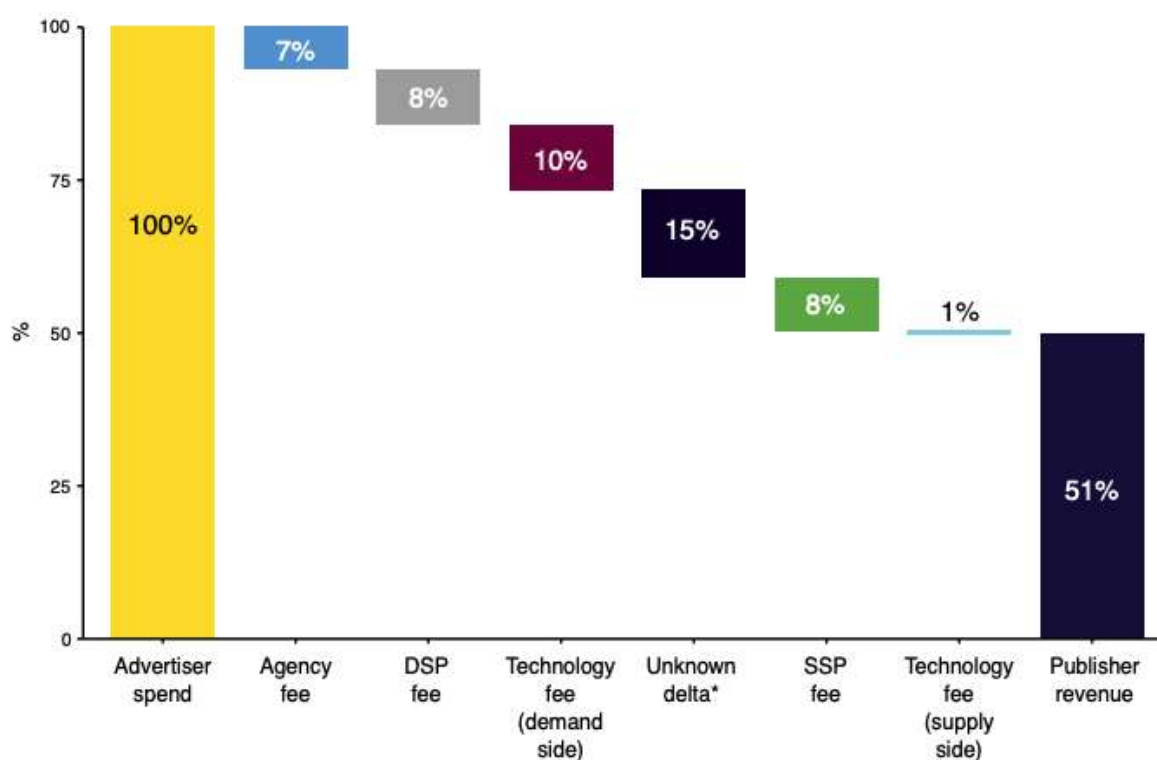


Figure 6: Illustration of the distribution of fees in the digital advertising supply chain. Source: ISBA/PwC Programmatic Supply Chain Transparency Study (2020).

Estimates of this “ad tech tax” vary between 40 and 60% of digital advertising spend⁴⁰³. A study by PwC for UK advertiser association ISBA found that only 51%

⁴⁰² Ritson M, ‘Ritson: P&G’s Marc Pritchard Has Made the Biggest Marketing Speech for 20 Years’ (*Marketing Week*, 31 January 2017) <<https://www.marketingweek.com/mark-ritson-marc-pritchard-viewability-fraud-speech/>> accessed 19 July 2022.

⁴⁰³ See ‘Guide to Programmatic Media (2014)’ (*World Federation of Advertisers*, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>> accessed 15

of digital advertising spend turns into publisher revenue (see figure 6). The report found that 7% of the fee went to advertising agencies, 8% to DSPs, 10% to other demand-side technology providers, 8% to SSPs, 1% to supply-side technology providers, and an unattributable 15% was an “unknown delta”, which the accounting firm could not attribute or explain⁴⁰⁴. IAB UK has suggested that the “unknown delta” may be accounted for by “foreign exchange translations, limitations in data sets and post-auction financing arrangements”⁴⁰⁵. However, a wider limitation of the available data on intermediary fees stems from the lack of independent sources on the efficiency and cost of intermediary services. The data that has been released, mostly by industry bodies, is also somewhat limited by the significant variation in estimated ad spend breakdowns between sources.

The significant costs of intermediation are important to consider as studies on the efficiency and efficacy of using personal data and profiling in advertising rarely compare outcomes for publishers or advertisers to alternatives where both tracking and intermediation costs are reduced. Consequently, the impacts of any reduction in online tracking should be accompanied by an analysis of whether or not it would or could reduce intermediation costs, and what the net reduction to advertisers would be in this scenario.

2.4.3 Efficacy and efficiency in relation to societal and environmental impact

This study has outlined how the digital advertising market today relies on the processing of large amounts of personal data to target and measure ads. This has an impact on European democracy and society, the environment and the privacy of EU citizens. There is limited evidence to suggest that there are sufficient gains for advertisers and publishers in terms of efficiency and efficacy to outweigh these societal impacts, especially in relation to ads bought directly from large platforms. It has proven difficult to generate credible counterfactual scenarios to today’s digital advertising ecosystem, as studies tend to either study short term impacts in the existing advertising market, which would likely look very different over time,

August 2022; Programmatic: Seeing Through the Financial Fog’ (*Association of National Advertisers (ANA)*, May 2017) <<https://www.ana.net/miccontent/show/id/ii-programmatic-financial-fog>> accessed 15 August 2022; ‘ISBA Programmatic Supply Chain Transparency Study’ (*ISBA*, 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁴⁰⁴ ISBA and others, *Programmatic Supply Chain Transparency Study*. (ISBA, 2020), p. 8, <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁴⁰⁵ ‘Fact Check: 10 Takeouts from Commentary on ISBA’s “Supply Chain Study”’ (*IAB UK*, 15 May 2020) <<https://www.iabuk.com/news-article/fact-check-10-takeouts-commentary-isbas-supply-chain-study>> accessed 20 June 2022.

or do not consider the significant costs of intermediation in contemporary digital advertising.

At least theoretically, many of the perceived benefits of the internet as a decentralised space for the free exchange of information can be linked to the role that digital advertising has played in funding online services and content. Digital advertising has enabled journalists and bloggers to fund their work independently from media conglomerates and the potential editorial oversight of their owners⁴⁰⁶. It has also provided the revenue that keeps basic online services such as file sharing, searching for information, and video streaming free to use for billions of users worldwide. On one level, free access facilitated by ad funding has undoubtedly led to benefits for consumers; users may access information sites allowing them to “to pick an appropriate activity or execute a task more efficiently” while saving time on “mundane tasks such as buying tickets, checking the weather, or getting driving directions”⁴⁰⁷. On another, financial barriers to education and publication have arguably been reduced by free access to online services; whereas funding historically acted as a de facto gatekeeper as to what opinions could be published on a platform, individuals from marginalised groups now have the opportunity to form communities and share their perspectives through free networking platforms. Indeed, the narrative that advertising is essential to “ensuring that the internet is available for the many, not just the few” is common among its proponents in industry⁴⁰⁸. Yet it is important to note that the benefits of open access are not necessarily contingent on the profiling and data processing that support the current predominant models of digital advertising. These benefits are associated with the ability to generate revenues through the sale of advertising inventory, not the ability to target ads based on profiling.

⁴⁰⁶ ‘Debate: Advertising Is the Best Way to Keep the Internet Free and Open’ (*IAB UK*, 29 January 2020) <<https://www.iabuk.com/news-article/debate-advertising-best-way-keep-internet-free-and-open>> accessed 23 June 2022.

⁴⁰⁷ Jaffe AB and others, *Innovation Policy and the Economy* (MIT Press, 2001) <<https://archive.org/details/innovationpolicy00mitp>> accessed 23 June 2022.

⁴⁰⁸ ‘Debate: Advertising Is the Best Way to Keep the Internet Free and Open’ (*IAB UK*, 29 January 2020) <<https://www.iabuk.com/news-article/debate-advertising-best-way-keep-internet-free-and-open>> accessed 23 June 2022.

2.5 Conclusion

Search advertising and social media advertising channels, where large platforms are market leaders, have grown at an extremely rapid rate over the past 10-15 years compared to the channel which directs the most advertising revenue to publishers (“other” display). Large platforms have also become key players in the “other” display channel by providing intermediary services for publishers and advertisers to buy and sell ads. As a result, a significant amount of digital advertising revenue flows towards large platforms (Google and Meta).

Data plays an essential role in digital advertising today. It is used for targeting and measuring advertising campaigns, and is often tied to common identifiers that enable companies to build up a picture of an individual’s behaviour across sites, apps, platforms and devices. Large platforms play an important role in this system. The distribution of data (and advertising-related revenue tied to it) is shifting due to moves by Google and Apple to restrict third-party tracking on their platforms. As a result, many in the industry are focusing on developing new systems and technologies to target and measure ads. A large amount of academic research has focused on demonstrating that the digital advertising status quo has significant impacts on privacy, democracy, society and the environment: this is summarised in this study. There is limited evidence to suggest that the efficiency and efficacy gains to advertisers and publishers of this system outweighs the societal impact.

Part B

To what extent is there an imbalance in the relationship between publishers/ advertisers and major platforms/ intermediaries?

3 Evolution and distribution of advertising spend across the digital advertising ecosystem

This section describes the trends in the share of advertising spend in the EU with reference to ten Member States: Bulgaria, Czechia, Germany, Greece, Spain, France, the Netherlands, Poland, Slovenia and Finland.

Available data at Member State level indicates that a significant amount of digital advertising spend flows towards large platforms (Google and Meta). This appears to be a common pattern across at least ten different countries, including in countries where the penetration of digital advertising is still developing.

3.1 Digital vs. traditional advertising

Table 6 displays the estimated digital and traditional spend data from the ten Member States selected in 2021, along with information on the proportion of spend as a percentage of Gross Domestic Product (GDP), and the rate of growth of spend between 2014 and 2021. As discussed in part A, data suggests that the rate of growth of digital advertising spend over this period far outpaced the growth of traditional advertising spend, reaching double- or triple-digit growth in all markets selected. Conversely, during the 2014-2021 period, traditional advertising spend contracted in Germany, Greece, Spain, France, the Netherlands and Finland. While traditional advertising spend grew in the remaining four Member States (Bulgaria, Czechia, Poland and Slovenia), digital advertising spend growth far exceeded it.

Across the ten Member States selected, digital advertising represents around 0.07-0.37% of GDP, and digital advertising spend as a proportion of total advertising spend ranged between 26-63%. The data points to Bulgaria and Greece being the market where digital advertising made up the smallest proportion of advertising spend, and the Netherlands the largest. Germany, Spain, France and the Netherlands are the only Member States in the selection where total digital advertising spend is greater than traditional advertising spend. Germany, France and the Netherlands are the countries with the largest digital

advertising spend and the Member States where digital advertising makes up the largest proportion of GDP.

The remainder of this section delves into the available evidence to analyse these trends at Member State level.

	EE A	BG	CZ	DE	EL	ES	FR	NL	PL	SI	FI
Digital advertising spend (2021, € million)	45,866	46	331	11,778	204	3,695	8,707	3,140	1,343	68	448
Digital advertising spend as % of GDP (2021)	0.30%	0.07%	0.14%	0.33%	0.11%	0.31%	0.35%	0.37%	0.23%	0.13%	0.18%
Traditional advertising spend (2021, € million)	43,494	131	666	10,528	569	3,594	7,056	1,872	1,420	119	809
Traditional advertising spend as % of GDP (2021)	0.28%	0.19%	0.28%	0.29%	0.31%	0.30%	0.28%	0.22%	0.25%	0.23%	0.32%
Digital advertising as a proportion of total advertising spend (2021)	51%	26%	33%	53%	26%	51%	55%	63%	49%	36%	36%
Digital advertising spend growth (2014-2021)	135%	498%	31%	103%	69%	261%	133%	133%	139%	119%	140%
Traditional advertising spend growth (2014-2021)	-14%	3%	21%	-20%	-53%	-8%	-13%	-12%	18%	10%	-20%

Table 6: Distribution of advertising spend in EEA (excluding Cyprus, Iceland, Lichtenstein, Luxembourg, and Malta), Bulgaria, Czechia, Germany, Greece, Spain, France, the Netherlands, Poland, Slovenia and Finland. Source: EEA data calculated using data from GroupM, Zenith, Omnicom, MagnaGlobal (see footnote 9); individual Member States data sourced from WPP (December 2021); GDP calculations based on Eurostat data.

3.2 Bulgaria

Bulgaria has the smallest digital advertising spend (€46 million) of all the member states in the study's selection. Additionally, digital advertising represents only

26% of local advertising spend and 0.07% of local GDP. Data from the Bulgarian Association of Communication Agencies (BACA) suggests that television is the largest advertising channel, representing 54% of ad spend in 2020⁴⁰⁹. Bulgaria's digital advertising market is the fastest growing in the selection, expanding 498% between 2014 and 2021.

According to IAB Bulgaria's 2020 AdEx study and data by local publisher Capital, local advertisers' programmatic advertising spend on Google was around €33 million in 2020 (50-60% of total national spend), around €21 million on Meta (30-40%) and less than €4 million on local publishers (1-7%)⁴¹⁰. Digital advertising spend on Google and Meta platforms increased by 22.9% and 28.1% respectively between 2019 and 2020, while it decreased by 0.9% on local publishers. It nonetheless also increased by 35.5% on local social media platforms. This suggests that in recent years, the majority of digital advertising growth has gone to Google, Meta and other social media platforms, rather than local publishers. Digital video display constitutes 38% of total display advertising spend (i.e. social media advertising plus "other" display); YouTube and Facebook make up around three quarters of spend in this segment, and Facebook around a quarter. Bulgarian video platforms meanwhile only make up 10-15% of video advertising spend.

3.3 Czechia

In comparison to the other Member States in the selection, digital advertising makes up a relatively small proportion of local advertising spend in Czechia (33%). As a proportion of GDP, traditional advertising spend in Czechia is one of the largest in the selection (0.28%), Finland being the first (0.33%). Recent research by local academics suggests that traditional advertising's strength can be attributed to TV advertising, which has grown at rates similar to digital advertising and remains a larger channel in terms of ad spend than digital advertising⁴¹¹.

Czechia is one of the few EU Member States where a publisher interviewed for this study indicated that a search engine other than Google was a "big gatekeeper" in the market and a "gate to the internet for many Czech people"⁴¹². The publisher

⁴⁰⁹ 'Големият Ръст На Дигиталната Реклама През 2020 Година Намалиява Общия Спад На Пазара | Медии | Новини От България и Света |' (*OFFNews*, 2021) <<https://offnews.bg/medii/golemiat-rast-na-digitalnata-reklama-prez-2020-godina-namaliava-obshti-765001.html>> accessed 17 May 2022.

⁴¹⁰ Пенкова С, 'Пазарът На Онлайн Реклама' (*Capital*, 26 November 2021) <https://www.capital.bg/biznes/media_i_reklama/2021/11/26/4269812_pazarut_na_onlain_reklama/> accessed 17 May 2022.

⁴¹¹ Konečný M and others, 'Analysis of the Czech Advertising Market and Its Main Players' (2022) 135 SHS Web of Conferences 01006, <https://www.researchgate.net/publication/358492727_Analysis_of_the_Czech_Advertising_Market_and_its_Main_Players>.

⁴¹² Publisher 4.

argued that publishers working with the platform Seznam only receive 30% of the revenue from ads placed on their sites. Larger publishers, they claimed, are able to gain larger proportions of revenue because their larger size gives them leverage to negotiate better terms.

3.4 Germany

At €11.8 billion in 2021 (up from €5.3 billion in 2014), digital advertising spend in Germany is the largest in the EEA in nominal terms and the third largest in terms of its contribution to local GDP (0.33%). Digital advertising spend in Germany represents 26% of total digital advertising spend in the EEA.

According to the German advertising federation, Zentralverband der deutschen Werbewirtschaft (ZAW)⁴¹³, Google, Meta and Amazon represented 80% of local digital advertising revenue in 2021. This is consistent with data from Statista, which indicates that Meta's share of social media advertising revenue was 80% in 2019, with Xing and Twitter each receiving just 5% of revenue, and that Google's share of search advertising revenue was 80%⁴¹⁴.

According to a survey of members of the German digital media association, Bundesverband Digitale Wirtschaft (BVDW), and the German advertising agencies association Organisation der Mediaagenturen (OMG)⁴¹⁵, 70% are concerned about having to rely more on Google and Meta for access to measurement data⁴¹⁶.

According to eMarketer, the retail industry is the sector that represents the largest proportion of digital advertising spend, having spent €2.26 billion in 2021, or 23.8% of total digital advertising spend. 69.2% of total digital advertising spend was spent on mobile ads in 2021, with retail once again representing the largest proportion of spend (27.7%).

⁴¹³ Scheppe M, 'Werbewirtschaft: 69 Prozent mehr Umsatz: Google und Co. gewinnen am Werbemarkt – Klassische Medien fallen zurück' (*Handelsblatt*) <<https://www.handelsblatt.com/unternehmen/it-medien/werbewirtschaft-69-prozent-mehr-umsatz-google-und-co-gewinnen-am-werbemarkt-klassische-medien-fallen-zurueck/27787322.html>> accessed 18 May 2022.

⁴¹⁴ 'Infografik: Immer mehr Geld für Werbung auf Facebook und Co.' (*Statista Infografiken*) <<https://de.statista.com/infografik/22976/ausgaben-fuer-social-media-werbung-in-deutschland/>> accessed 18 May 2022.

⁴¹⁵ The BVDW and OMG are made up of 39 companies, representing 90% of agency digital advertising spend in Germany.

⁴¹⁶ 'Grosse Trends in Online Media, FOMA-Trendmonitor' (*BVDW*, 2021) <https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/foma/FOMA_Trendmonitor_2021.pdf>.

3.5 Greece

Traditional advertising spend in Greece contracted by 53% between 2014 and 2021. During that time, total digital advertising spend grew 69%, meaning it had the slowest digital advertising spend growth of the countries in the selection. Digital advertising remains a relatively small part of local advertising spend, at just 26% of the total.

3.6 Spain

Of the larger Member States in terms of digital advertising spend in the selection (including Germany, France and the Netherlands), Spain saw the most growth between 2014 and 2021 (261%).

According to Spain's local competition authority, the Comisión Nacional de los Mercados y la Competencia (CNMC)⁴¹⁷, Google's share of the search advertising market was 90% in 2019 and Meta's share of the "display advertising" market was over 40%. The "open" display market (i.e. the inventory of publishers with a largely national audience, which is sold to advertisers primarily through intermediaries) meanwhile represents 41-42% of the "display advertising" market. According to the CNMC, the share of the rest of the "display advertising" market (under 40%) is held by other platforms such as Amazon, YouTube, Twitter, Spotify and LinkedIn. The CNMC study indicates that while large platforms account for about a quarter of the total digital advertising market, publishers only make up about a fifth. Additionally, while large platforms' revenues from digital advertising are growing at annual rates that may exceed 25%, publishers' revenues from the open display market are only growing at annual rates of 10-20%, meaning their relative share of the market is decreasing.

Findings from the CNMC also suggest that Google has a large market share throughout the different parts of the digital advertising supply chain in Spain. The CNMC estimated that Google represents over 70% of advertiser ad server market revenue in Spain (with the next largest, Sizmek-Amazon, representing less than 20%), over 70% of the publisher ad server market revenue (with Smart AdServer representing less than 20%), 60% of demand-side platform (DSP) market revenue (with The Trade Desk and Amazon representing less than 20% each), and over 50% of supply-side platform (SSP) market revenue.

⁴¹⁷ 'E/CNMC/002/2019 Study on the Competition Conditions in the Online Advertising Sector in Spain' (Comisión Nacional de los Mercados y la Competencia, 7 July 2021) <https://www.cnmc.es/sites/default/files/3696007_1.pdf>.

3.7 France

France is the second largest Member State in terms of digital advertising spend in the EEA (€8.7 billion in 2021, up from €3.4 billion in 2014), representing 55% of total advertising spend.

According to the French competition authority, *Autorité de la Concurrence*, (ADLC)⁴¹⁸, Google's share of the local search advertising market was 70% in 2019. Data from *Syndicat des Régies Internet (SRI)*⁴¹⁹ estimates that Google, Meta and Amazon represent 67% of digital advertising spend in France, a proportion that has grown steadily over the last three years (their share of spend was 65% in 2019). In 2021, growth in spend towards these three platforms was responsible for 73% of the total growth in local digital advertising spend. Google, Meta and Amazon's revenues increased by 27% in 2021, whereas the rest of the market in terms of digital advertising spend only grew by 19%. Programmatic advertising represented 64% of digital advertising spend in 2021, having grown from 58% in 2019. Digital audio is currently one of the fastest growing digital advertising channels in France, growing 58% between 2020 and 2021 to €48 million.

During an interview as part of this study, French advertiser association *Union des Marques* noted that local advertisers had a "hate and love relationship" with large platforms. They suggested that advertisers enjoy the use of platforms' "technologically advanced solutions at a low cost" and "personalisation at scale" but lack transparency over measurement. They furthermore argued that platforms' "domination of the market, [...] implies setting prices without negotiation" in turn "creating an environment in which you cannot operate without them".

3.8 The Netherlands

Digital advertising spend in the Netherlands is the third largest in the selection in nominal terms, but the largest in relative terms, constituting 63% of local advertising spend and 0.37% of local GDP. Search advertising is the largest digital advertising channel in the Netherlands, representing 46% of spend.

⁴¹⁸ 'Avis N° 18-A-03 Du 6 Mars 2018 Portant Sur l'exploitation Des Données Dans Le Secteur de La Publicité Sur Internet' (*Autorité de la Concurrence*, 6 May 2018)

<<https://www.autoritedelaconcurrence.fr/sites/default/files/2019-05/18a03.pdf>>.

⁴¹⁹ Wyman O, 'FY 2021 Review (27th Ed)' (SRI France, 2021) <https://www.sri-france.org/wp-content/uploads/2022/02/27%C2%B0Observatoire-E-Pub-FY-2021_VF030222_ENG.pdf>.

According to data from Statista, Meta represented 85% of social media advertising revenue in the Netherlands in 2021⁴²⁰, and Google represented 90% of search advertising revenue⁴²¹. Global publishers (including large platforms) are the destination of 70% of digital advertising spend, with local publishers receiving the remaining 30%. The ad revenue of local publishers is decreasing rapidly. In 2016, they represented 43% of the market. This is consistent with the data in table 6, which shows that traditional advertising spend decreased by 36% between 2014 and 2021.

According to a separate piece of research from Deloitte⁴²², the majority of programmatic advertising in the Netherlands in 2020 was bought through open auctions (68%), with 24% bought through private auctions, and the remaining 7% through programmatic guaranteed and preferred deals. The share of digital advertising spend has been growing quickly and represented 60% of spend in 2020, up from 5% in 2012.

3.9 Poland

Traditional and digital advertising spend in Poland is amongst the smallest in the selection as a proportion of local GDP, representing just 0.25% and 0.23% of local GDP respectively. Digital advertising spend in Poland is the third-fastest growing in the selection, expanding 139% between 2014 and 2021.

According to research by local publisher Interaktywnie.com⁴²³, Google held a 75% share of the search advertising market in Poland in 2020. Data from Statista⁴²⁴ suggests that Meta held a 78% share of the social media advertising market in Poland in 2021.

⁴²⁰ 'Social Media Advertising - Netherlands' (*Statista Market Forecast*)

<<https://www.statista.com/outlook/dmo/digital-advertising/social-media-advertising/netherlands>> accessed 14 June 2022.

⁴²¹ 'Search Advertising - Netherlands' (*Statista Market Forecast*)

<<https://www.statista.com/outlook/dmo/digital-advertising/search-advertising/netherlands>>

accessed 14 June 2022; 'Digital Advertising Spend 2019 The Netherlands' (*Deloitte & IAB Nederland*, May 2020) <https://gertkoot.files.wordpress.com/2020/05/ad_spend_study_2019.pdf>.

⁴²² 'Digital Advertising Spend 2020 The Netherlands' (*Deloitte & VIA*, April 2021)

<<https://view.deloitte.nl/rs/502-WIB-308/images/Digital-Ad-Spend-study-2020.pdf>>.

⁴²³ 'Raport: Agencje SEO i Marketing w Google. Dane, Analizy, Nowości, Porady Ekspertów'

(*interaktywnie.com*, 25 May 2020) <<https://interaktywnie.com/biznes/newsy/biznes/raport-agencje-seo-i-marketing-w-google-dane-analizy-nowosci-porady-ekspertow-260071>> accessed 14 June 2022.

⁴²⁴ 'Poland: Social Media Market Share 2021' (*Statista*)

<<https://www.statista.com/statistics/979859/poland-social-media-market-share/>> accessed 14 June 2022.

3.10 Slovenia

With a size of €68 million, Slovenia is the second smallest Member State in terms of digital advertising spend in the study's selection. Digital advertising spend also represents one of the smallest proportions of GDP, at just 0.13%, and just 36% of total local advertising spend. Digital advertising spend in Slovenia is nonetheless one of the fastest growing in the selection, expanding by 119% between 2014 and 2021. According to data by IAB Slovenia⁴²⁵, local media represented 27% of local digital advertising spend in 2020, whereas foreign media (which includes large platforms) represented 56%. While YouTube and Meta's local digital advertising revenues grew by 35% and 10% respectively in 2020, those of local media grew by just 1%, suggesting that large platforms' relative share of digital advertising spend is growing. During an interview as part of this study, IAB Slovenia suggested that the digital advertising revenues of local media are growing slower than the revenues of large platforms. Nonetheless, in 2021, social media advertising was the smallest digital advertising channel (15%), making it the smallest Member State in terms of social media advertising spend in the selection in relative terms.

According to a survey by Slovenian advertising agency iPROM⁴²⁶, at the beginning of 2020, local advertisers planned to allocate 28% of their total budgets to "display advertising"⁴²⁷, 20% to social media advertising, and 18% to search advertising⁴²⁸. The advertisers polled by iPROM noted that their main reason for using digital advertising was its effectiveness/efficiency (71%), accurate metrics/measurement (59%), compliance with data protection regulation (59%) and effective targeting (55%).

3.11 Finland

Traditional advertising spend in Finland contracted by 20% between 2014 and 2021. During that time, digital advertising spend grew by 140%. Digital advertising is nonetheless just 36% of total advertising spend in Finland.

⁴²⁵ 'ADEX 2020' (*IAB Slovenija*)

<<https://www.iab.si/showpdf?file=https://www.iab.si/files/default/baza-znanja/2020-2021/AdEx2020%20IAB.pdf>> accessed 20 May 2022.

⁴²⁶ 'Slovenian Advertisers Will Again Spend the Most on Display Advertising' (*iPROM*, 25 May 2020)

<<https://iprom.eu/slovenian-advertisers-will-again-spend-the-most-on-display-advertising/>> accessed 24 May 2022.

⁴²⁷ Here to be understood as synonymous with "other" display.

⁴²⁸ It is important to note that iPROM's study was undertaken at an early stage of the COVID-19 pandemic, at the beginning of 2020. As such it is possible that advertisers' investment plans may have changed significantly throughout the year.

When interviewed as part of this study, local advertising association Marketing Finland said that advertisers feel like Google and Meta are not sufficiently transparent. They noted that advertisers have begun suspecting that the ad services provided by both companies are not as effective as they claim, because the data provided does not align with advertisers' own data. According to the association, this has led to a "lack of trust" in both companies and advertisers which have a "higher level of trust" in local platforms, especially in relation to helping advertisers apply self-regulatory standards (e.g. to ensure that ads for alcohol or certain food are not shown to children).

3.12 Conclusion

Although the availability of data across the Member States selected varies, it is clear that large platforms such as Google and Meta play a key role in digital advertising in all of them. This is the case both in Member States where digital advertising is relatively advanced (such as France, Germany, the Netherlands and Spain), and Member States where the penetration of digital advertising is still developing (such as Bulgaria, Czechia, Poland and Slovenia).

4 Advertisers' and publishers' experiences

This section describes advertisers' and publishers' experiences with digital advertising with reference to interviews undertaken between January and April 2022 with nine advertisers and eight publishers, including five small- and medium-sized enterprises (SME) advertisers and three SME publishers, as well as several relevant trade associations.

As noted in the interview methodology (section 4.6), interviewees were given the option to speak on an anonymous basis so as to be able to gather as much honest and "unfiltered" feedback as possible. Out of nine advertisers and eight publishers interviewed, 12 requested anonymity for all or part of the interviews. See table 7 in the interview methodology (section 4.6) for an overview of the advertisers and publishers interviewed for the study.

This section begins by describing the benefits of digital advertising identified by advertisers and publishers, to give an overview of their main motivations for using it. It then looks at how advertisers and publishers describe their relationships with major platforms and digital advertising intermediaries. The section then describes key issues that publishers and advertisers identified which are related to the way the current digital advertising ecosystem functions.

Key findings

Compared to traditional offline advertising (e.g. TV), advertisers feel that digital advertising is an easier and cheaper way to advertise to a large number of people. However, this can make it difficult for publishers to compete for digital advertising revenue because large platforms generally offer wider reach for advertisers (due to network effects) and lower prices (due to economies of scale).

There is a perception that the value of digital advertising is higher when it can be targeted based on detailed knowledge about the individual who is likely to view the ad (usually linked to profiling based on personal data). However, there appears to be limited empirical evidence to support this notion. Publishers said that this allows them to charge a premium to advertisers, although this also puts them at a competitive disadvantage compared to large platforms that have the ability to collect more data.

Digital advertising campaigns can be analysed and adjusted in real-time to optimise return-on-investment (ROI), although many advertisers have doubts about the accuracy of the statistics provided to them by the companies they buy advertising services from (particularly large platforms). Advertisers and publishers both feel that the digital advertising ecosystem is not transparent enough, especially in relation to the use of personal data, performance metrics and fees.

Advertisers and publishers both described feeling a sense of “dependency” on large platforms to buy and sell digital advertising and they often used negative terms to describe the relationship (including “abusive”, “aggressive”, “love/hate relationship (without the love)” and “frenemies”). Most said they would like to see more alternative options in the digital advertising ecosystem. When asked about their relationship with intermediaries that provide ad tech services, respondents (particularly publishers) noted that they provide essential functions but complained about high costs and complexity.

4.1 Benefits of digital advertising for advertisers and publishers

Compared to traditional offline advertising (e.g. TV), advertisers feel that digital advertising is an easier and cheaper way to advertise to a large number of people. However, this can make it difficult for publishers to compete for digital advertising revenue because large platforms generally offer wider reach for advertisers (due to network effects) and lower prices (due to economies of scale).

Digital advertising campaigns can be analysed and adjusted in real-time to optimise return-on-investment (ROI), although many advertisers have doubts

about the accuracy of the statistics provided to them by the companies they buy advertising services from (particularly large platforms).

There is a perception that the value of digital advertising is higher when it can be targeted based on detailed knowledge about the individual who is likely to view the ad (usually linked to profiling based on personal data). However, there appears to be limited empirical evidence to support this notion.

Publishers said nonetheless that this allows them to charge a premium to advertisers, although several interviewees indicated that they expected digital advertising to use less personal data in the future.

4.1.1 Ability to reach large audiences online

One of the most important benefits of digital advertising identified by respondents was the ability to present ads to a large number of individuals in environments where they are increasingly spending a large proportion of their time. As one advertiser said, “digital is where customers are [...] so we need to be there”⁴²⁹. This provides advertisers with the ability to reach large numbers of people with their messages, at a scale that can be significantly bigger than traditional offline advertising channels.

In this environment, platforms with a large user base (often described in the industry as “walled gardens”) are particularly attractive to advertisers as they offer the ability to reach a large number of people through a single ad or campaign. All advertiser respondents suggested that one of the key benefits of advertising on Google or Meta platforms was their large user base. Small advertisers with limited advertising budgets and technical resources find this particularly useful. One small advertiser explained that “what is awesome with Google is that you cover basically everyone, because everyone is on Google every day”⁴³⁰.

From a publisher perspective, one interviewee explained that the shift towards people spending more time online has increased the importance of revenues from digital advertising and subscriptions to replace revenues from physical sales (e.g. newspapers, magazines), as these have been on the decline⁴³¹. A 2021 Accenture report commissioned by Google found that revenues from the sale of newspapers in Western Europe declined by 17% between 2003 and 2019⁴³². Although most

⁴²⁹ Advertiser 1.

⁴³⁰ Advertiser 8.

⁴³¹ Publisher 6.

⁴³² ‘Western Europe News Media Landscape Trends’ (Accenture, 2021) <https://newsmediaanalysis.s3-ap-southeast-2.amazonaws.com/accenture_analysis/WesternEuropeNewsMedia.pdf>.

publishers talked about monetising digital content through a mixture of advertising and subscriptions, two publishers suggested that it can be significantly more difficult for online publications to grow revenues through subscriptions than advertising⁴³³. According to publisher association News Media Europe, although several large national publishers have seen success in their subscription strategies, “there’s a form of saturation in the market because at the end of the day people are only willing to take out so many subscriptions”. Growing subscription revenues was also viewed as a potential barrier to increasing the reach of news due to “paywalls” limiting people’s access to content. Concerns were also raised that this could have a negative impact on democracy. One publisher suggested that if most news content in their country was behind a paywall, it “would leave a large part of the population in a kind of news desert” with no access to quality journalism and news content⁴³⁴. As a result, digital advertising remains an important revenue stream for publishers.

4.1.2 Targeting methods

Advertisers and publishers also said that a key benefit of digital advertising is the ability to use data to target ads towards people who are likely to be interested in their products and services⁴³⁵. “Success [in digital advertising campaigns] is the ability to reach the target audience with your message”⁴³⁶, said one small advertiser. This perception is supported by a 2022 survey by audience measurement, data and analytics company Nielsen, which found that advertisers thought that audience targeting was the most important factor influencing campaign performance⁴³⁷.

Publishers stated that they are able to sell advertising inventory at a higher price if they can persuade buyers that they know something about the person who is going to view the ad. Publishers typically use personal data to draw inferences which they believe can increase the perceived value of the ad inventory they are selling. One large publisher suggested that this can increase the price of advertising by 50%⁴³⁸. News Media Europe estimated that publishers generate “two to three times” more revenue when they are able to connect personal data to ad inventory. However, some publishers were cynical about whether the perceived additional value that advertisers attribute to personal data in this

⁴³³ Publishers 1 and 6.

⁴³⁴ Publisher 6.

⁴³⁵ Advertisers 1, 3 and 4.

⁴³⁶ Advertiser 3.

⁴³⁷ ‘Global Annual Marketing Report 2022’ (*Nielsen*, 12 April 2022)

<https://annualmarketingreport.nielsen.com/wp-content/uploads/sites/16/pdf/full_report_1651149101_1118689979.pdf> accessed 2 June 2022.

⁴³⁸ Publisher 1.

context is justified. When asked why advertisers attribute more value to inventory that was linked to personal data, one large publisher said “I am not sure why, but this is what advertisers want. You should ask them!”⁴³⁹. Another large publisher suggested that although they had done some analysis for specific advertisers that showed lifts in brand awareness and higher engagement when using personal data for ad targeting, “we have to be honest though that it often does not work”⁴⁴⁰. The same publisher suggested that the quality of personal data is often poorer than many advertisers assume: “data based on registered users and what they have told us is pretty good quality and reliable, but when you start to have algorithmically estimated age and gender it gets poor quite fast. For more complicated predictions like ‘intends to buy a car’, this drops exponentially”⁴⁴¹.

Despite the perception shared by advertisers and publishers that personal data increases the value of digital advertising, there is little empirical data to support this notion (for more discussion on this, see section 2). When asked why they saw value in being able to target ads to people based on their personal data, advertiser interviewees tended to point to the general benefits of digital advertising (e.g. low cost, ability to reduce waste by measuring and optimising performance in real-time) rather than specific evidence related to the use of personal data. This signals that because the use of personal data has become an inherent part of digital advertising, many advertisers may (historically at least) have been unable to separate out the specific benefits that this feature brings above and beyond the more general benefits of advertising online compared to offline. However, there is a sense that this is now changing, as Google and Apple’s restrictions on third-party data collection are forcing companies to assess the value of maintaining access to personal data either by developing and investing in new identity solutions or changing the partners they work with. Because these approaches could require change (at a strategic and/or operational level) and therefore cost, many large advertisers indicated that they are in the process of carrying out due diligence on the use of personal data in digital advertising (many of them for the first time). As a result, some are experiencing a “lightbulb” moment. One large advertiser told us that they felt the use of personal data for advertising needed to happen in a “light post campaign way, not in a very deep and invasive way”. They said “I do not need to know every website you have been to for the last six months just to figure out if I should serve an ad to you – that is too much information for the job”⁴⁴². Another large advertiser said they felt the market shift towards less third-party data was “a good change” that they were “embracing”⁴⁴³.

⁴³⁹ Publisher 1.

⁴⁴⁰ Publisher 5.

⁴⁴¹ Publisher 5.

⁴⁴² Advertiser 2.

⁴⁴³ Advertiser 4.

Respondents' answers regarding the data that they thought was most important for targeting based on profiling varied. Although several publishers noted the importance of demographic data (age, gender, socio-economic status)⁴⁴⁴, several advertisers noted that interest data was often more important to them⁴⁴⁵. One advertiser noted that demographic data "tells you nothing" because people with the same age and gender can have very different interests⁴⁴⁶. This suggests that there is a potential disconnect between what publishers think advertisers want in terms of data, compared to what advertisers actually say they need. Several advertisers interviewed for this study emphasised that they do not require "granular targeting"⁴⁴⁷ for their digital advertising campaigns (i.e. overly complex and precise targeting criteria is not essential). One large advertiser said that more and more often they "get rid of targeting"⁴⁴⁸ based on personal data, while another said they do not use targeting based on profiling anymore because they "do not want to chase people across the internet"⁴⁴⁹. Small advertisers, however, described targeting based on profiling as important⁴⁵⁰, albeit largely in order to avoid showing ads to people who are not interested (see section 4.1.4).

Overall, it is ultimately unclear how much of these perceptions of the value of data is based on hard evidence. Although advertisers and publishers interviewed were categorical in their convictions of the effectiveness of advertising based on profiling, none provided data to support these claims. As discussed in section 2.4.1, although some studies suggest that advertising based on profiling can lead to higher revenues for publishers, comparisons between the current model and models that rely on less personal data are ultimately difficult to make. Furthermore, as discussed in greater detail in section 4.1.3, advertisers interviewed for this study generally feel as though their ability to accurately measure the effectiveness of campaigns is limited. This suggests that advertisers and publishers believe that digital advertising based on profiling helps them secure better outcomes, despite not having a full view of how effective it is, including in comparison to alternative models⁴⁵¹.

4.1.3 Measurement

Measurement is typically a high priority for both advertisers and publishers. Advertisers said they use measurement data to help them optimise and adjust

⁴⁴⁴ Publishers 1, 2, 5 and 8.

⁴⁴⁵ Advertisers 1, 2, 3 and 6.

⁴⁴⁶ Advertiser 1.

⁴⁴⁷ Advertisers 1, 2 and 5.

⁴⁴⁸ Advertiser 1.

⁴⁴⁹ Advertiser 5.

⁴⁵⁰ Advertisers 3, 6 and 7.

⁴⁵¹ See section 5 for a discussion of the available evidence on the effectiveness of alternative models.

their campaigns⁴⁵². For many, this is a key advantage of digital advertising compared to traditional, offline methods. Indeed, one advertiser noted that they were spending less on traditional outdoor advertising because “you do not get a view of impact, so it is not worth it”⁴⁵³. Several interviewees suggested that, for large advertisers especially, it was more important to collect data for measurement than for targeting, although most respondents would prefer to have both⁴⁵⁴. One publisher said that “if you do not have measurement, then targeting is not that useful”⁴⁵⁵.

Publishers use measurement data to attract advertising revenue by demonstrating the efficacy of advertising on their content⁴⁵⁶. One publisher argued that “if you don’t do measurement, don’t start [doing digital advertising]”⁴⁵⁷. Another publisher said that measurement was “kind of mandatory” because of advertisers’ focus on efficiency of media spend (i.e. making sure that their campaigns are optimised to achieve their objectives)⁴⁵⁸. Respondents furthermore noted that the use of unique identifiers was crucial to count how many times a single user saw an ad⁴⁵⁹.

However, in reality, advertisers often said they find it difficult to rely on the accuracy of the measurement data they have access to today – as described in section 4.3.

4.1.4 Cost

The combination of targeting (see 4.1.2) and measurement (see 4.1.3) was seen by many advertisers (particularly SMEs) as advantageous in terms of cost because they believe it reduces potential waste in advertising spend⁴⁶⁰. One small advertiser said this is important because “we lose money if we show ads to people who aren’t interested”⁴⁶¹. The ability to attribute conversions⁴⁶² to specific campaigns enables small advertisers to understand what channels and types of campaign bring the most value to their company. One small advertiser said “attribution is really important because, when you’re a small company, you don’t

⁴⁵² Advertisers 1 and 9.

⁴⁵³ Advertiser 9.

⁴⁵⁴ Advertisers 1, 2 and 5; Publishers 2 and 6.

⁴⁵⁵ Publisher 5.

⁴⁵⁶ Publisher 6.

⁴⁵⁷ Publisher 8.

⁴⁵⁸ Publisher 1.

⁴⁵⁹ Publishers 3 and 6.

⁴⁶⁰ Advertisers 1, 3, 6 and 7.

⁴⁶¹ Advertiser 6.

⁴⁶² Conversions can be defined depending on the campaign (e.g. signing up for a subscription to an online service, filling out a form, buying a product, requesting a meeting with a sales team)

have millions of euros, so you want to spend your money wisely, but it's not always easy to know which of your campaigns has worked or not"⁴⁶³.

More generally, the cost of digital advertising is seen to be lower than traditional offline methods such as TV. Two small advertisers mentioned that digital advertising was the cheapest and easiest way to reach their target audience⁴⁶⁴. One of them noted that ensuring that their ads reach the right people was important from an efficiency standpoint, because they do not have a large advertising budget. One advertiser said that they find the ROI of digital advertising is higher than traditional advertising, because it is more effective at promoting brand awareness and sales⁴⁶⁵.

4.2 The relationship between publishers and advertisers, major platforms and intermediaries

4.2.1 Common issues identified by advertisers and publishers in relation to large platforms

When asked how they would describe their relationship with large platforms, nearly all advertisers and publishers, large and small, used negative terms such as "abusive"⁴⁶⁶, "aggressive"⁴⁶⁷, "love/hate relationship"⁴⁶⁸, "love/hate relationship, without the love"⁴⁶⁹, "not a love relationship"⁴⁷⁰, "asymmetric relationship"⁴⁷¹, "frenemies"⁴⁷², or noted that the relationship was "broken" and "painful"⁴⁷³. Despite this, respondents continue to work with these platforms, sometimes exclusively. Most of the small advertisers interviewed for this study said they spend at least 80% of their digital advertising budget with Google and Meta⁴⁷⁴, with two saying that these platforms account for 100% of their digital advertising spend⁴⁷⁵. One large advertiser said that nearly half of their advertising spend went to large platforms, split evenly across Google, Meta and Amazon, and

⁴⁶³ Advertiser 3.

⁴⁶⁴ Advertisers 3 and 7.

⁴⁶⁵ Advertiser 5.

⁴⁶⁶ Publisher 3.

⁴⁶⁷ Advertiser 1.

⁴⁶⁸ Advertiser 9.

⁴⁶⁹ Publisher 5.

⁴⁷⁰ Publisher 7.

⁴⁷¹ News Media Europe, Federation of European Data and Marketing.

⁴⁷² Publisher 1.

⁴⁷³ Advertiser 4.

⁴⁷⁴ Advertisers 3, 6 and 7.

⁴⁷⁵ Advertisers 6 and 7.

this had grown significantly over time⁴⁷⁶. Qualitative research based on interviews with advertisers undertaken by Jigsaw Research on behalf of the UK Competition and Markets Authority (CMA) similarly found that “despite [...] growing resentment over price increases, [Google and Meta] were still seen as much better options [by advertisers] than any other providers – and respondents did not want to consider switching to other providers. That said, there was also some perception that there simply weren’t any comparable alternatives”⁴⁷⁷.

Several common themes emerged among advertisers and publishers when talking about their relationship with large platforms, mostly linked to concerns about dependency, competition and future shifts in the way data is collected. The issues discussed below chiefly concern the relationships advertisers and publishers have with Google and Meta. Although three advertisers noted that they used Amazon’s advertising services⁴⁷⁸, most interviewees focused on Google and Meta as their key advertising partners.

4.2.1.1 Concerns about dependency

Advertisers and publishers both described feeling a sense of “dependency”⁴⁷⁹ on large platforms to buy and sell digital advertising.

- **Advertisers** said that they feel like they “have to” to work with Google and Meta⁴⁸⁰ to buy digital advertising because of their large size even though they feel unable to negotiate trading terms with these companies. One advertiser described Google and Meta’s approach to doing business with them as “take it or leave it”⁴⁸¹. French advertiser association Union des Marques said that advertisers have a “hate and love relationship” with large platforms, whereby they appreciate the use of platforms’ services, but complain that platforms’ “domination of the market [...] implies setting prices without negotiation”⁴⁸². A survey undertaken by Amnesty International and Global Witness suggests this feeling is widespread among small advertisers. It found that 69% of small advertisers in France and Germany were “uncomfortable with [Meta} and Google’s influence” and “felt they had no option but to advertise with them due to their dominance

⁴⁷⁶ Advertiser 4.

⁴⁷⁷ ‘Digital Advertising Services Qualitative research report’ (*Jigsaw Research and the Competition and Markets Authority*, June 2020)

<https://assets.publishing.service.gov.uk/media/5efb3fded3bf7f769d2695af/Digital_Advertising_Services_Research.pdf>.

⁴⁷⁸ Advertisers 1, 4 and 5.

⁴⁷⁹ Advertisers 1 and 2.

⁴⁸⁰ Advertisers 1 and 2.

⁴⁸¹ Advertiser 5.

⁴⁸² See section 3.7 for more detail.

of the industry”⁴⁸³. That said, it is worth noting that although this survey has a relatively large sample (617 SMEs), it may not be representative of how SMEs in Member States other than France and Germany feel.

- **Publishers** described a situation where they feel they need to build a constructive partnership with Google because of its large market share in different parts of the programmatic advertising market⁴⁸⁴, despite perceived concerns about anti-competitive behaviour. Three publishers explicitly said that not working with Google would likely result in loss of revenue for them⁴⁸⁵. A number of different concerns were raised by the publishers interviewed, including:
 - Perceived limits on interoperability between services provided by Google and others. Two publishers suggested this incentivises advertisers and publishers to use Google services throughout their ad tech stacks, thereby limiting competition. One publisher said that they had to abandon working with a preferred, non-Google intermediary because a lack of interoperability with Google services and data caused them to lose advertising revenue⁴⁸⁶.
 - High fees charged by Google for different services provided⁴⁸⁷.
 - One small publisher complained that Google’s position enables it to make unilateral changes to its advertising tools without giving all publishers sufficient notice to adapt their business practices, sometimes resulting in loss of revenue⁴⁸⁸.

4.2.1.2 Calls for a more diverse, competitive ecosystem

The majority of advertisers and publishers said or implied that they would like to see more alternative options in the digital advertising ecosystem beyond Google and Meta. Small advertisers were particularly concerned about lack of competition, with one calling for digital advertising to have “less monopolies”⁴⁸⁹, and another

⁴⁸³ ‘France/Germany: Small businesses want EU to get tough on Google and Facebook’s invasive advertising – new research’ (*Amnesty International*, 17 January 2022) <<https://www.amnesty.org/en/latest/news/2022/01/france-germany-small-businesses-want-eu-to-get-tough-on-google-and-facebooks-invasive-advertising-new-research/>>.

⁴⁸⁴ According to the UK competition authority, the CMA, in the UK, Google has a “controlling a share of [90-100]% of the publisher ad server segment, [80-90]% of the advertiser ad server segment and shares of [50-60]% in supply-side platforms (SSPs) and [50-60]% in demand-side platforms (DSPs)”. ‘Online Platforms and Digital Advertising - Market Study Final Report’ (*Competition and Markets Authority*, 2020), p. 19, <https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf>. See also section 1.2.2.4.

⁴⁸⁵ Publishers 1, 3 and 6.

⁴⁸⁶ Publishers 3 and 6.

⁴⁸⁷ Publisher 5.

⁴⁸⁸ Publisher 7.

⁴⁸⁹ Advertiser 3.

saying that Google should not be allowed to have a “monopoly” in any part of the market⁴⁹⁰. A large advertiser suggested that sellers of ad inventory should not be allowed to also provide intermediary services⁴⁹¹. The European Publishers Council, which describes itself as a high-level group of chairpersons and CEOs of publishers, similarly noted that “Google dominates digital advertising. They dominate the buy side and the sell side, and they are in a unique position to be able to leverage the knowledge that they have for their financial advantage”. One publisher called for “Google’s dominance” to be reduced⁴⁹², another called for Google to be regulated like a “utility” with “mechanisms that enable competition”⁴⁹³, and another said that reliance on large platforms should be reduced, and that regulators should not “let them define market conditions”⁴⁹⁴. One small publisher called for laws to act as a “counterweight” to the power of Google and Meta⁴⁹⁵ and another argued that digital advertising would be improved if it was “less concentrated in the hands of a few large players”⁴⁹⁶.

A bill introduced in the US Senate aims to somewhat alleviate advertisers’ and publishers’ concerns with regards to large platforms’ vertical integration in the market⁴⁹⁷. The Competition and Transparency in Digital Advertising Act (CTDA) proposes to prohibit companies that provide digital advertising services from owning more than one intermediary service if they process more than \$20 million in ad transactions. It would (1) prohibit ad exchange owners from owning supply-side platforms (SSPs) or demand-side platforms (DSPs), (2) prohibit owners of SSPs from owning DSPs (and vice versa), and (3) prohibit sellers and buyers of advertising space from owning DSPs and SSPs (except to sell their own advertising space).

4.2.1.3 Concerns about future limits on third-party tracking

As outlined in section 1.3.1.2, the role of identity in digital advertising is changing due to moves by Google and Apple to restrict third-party tracking within their browser and mobile ecosystems. Advertisers and publishers said they feel that this is making it harder to get the transparency they would like regarding measurement and targeting, with one of them noting that they were “losing ability to track the results of [their digital] campaigns”⁴⁹⁸. Some publishers suggested

⁴⁹⁰ Advertiser 7.

⁴⁹¹ Advertiser 1.

⁴⁹² Publisher 3.

⁴⁹³ Publisher 5.

⁴⁹⁴ Publisher 6.

⁴⁹⁵ Publisher 8.

⁴⁹⁶ Publisher 7.

⁴⁹⁷ Competition and Transparency in Digital Advertising Act, SIL22678, 117th Cong. (2022) <<https://www.lee.senate.gov/services/files/7384B096-04C3-4A3A-9796-80D22483026F>>.

⁴⁹⁸ Advertisers 1 and 4.

that this was making it more difficult for them to use digital advertising to replace declining revenues associated with print sales and print advertising⁴⁹⁹.

4.2.2 Common issues identified by advertisers and publishers in relation to intermediaries

When asked about their relationship with intermediaries⁵⁰⁰ that provide ad tech services, respondents (particularly publishers) noted that they provide essential functions but complained about high costs and complexity. In some cases, advertisers and publishers, particularly small ones, noted that cost and complexity issues associated with the use of intermediaries had pushed them towards using the services of large platforms instead.

4.2.2.1 Essential for publishers but high costs involved

Publishers said that they felt that working with intermediaries was essential. Two publishers (one large and one small) said that this is because they do not have the resources to offer programmatic advertising to advertisers without using intermediaries⁵⁰¹. However, several publishers raised concerns that using intermediaries can often involve high costs. Two publishers referenced the 2020 industry study discussed in section 2.4.2 which concluded that 50% of programmatic advertising spend goes to intermediaries and agencies^{502, 503}, and another publisher mentioned a study by The Guardian which found that the newspaper only received 30% of money spent by advertisers to place ads on the site^{504, 505}. Three advertisers highlighted issues related to high cost and complexity when working with intermediaries⁵⁰⁶. Publisher association News Media Europe described the programmatic advertising ecosystem as a “black box” that prevents publishers from knowing “whether they get value for their ad space”.

⁴⁹⁹ Publishers 1 and 2.

⁵⁰⁰ For a more detailed definition and description of ‘intermediaries’, see section 1.2.2.4.

⁵⁰¹ Publishers 1 and 7.

⁵⁰² ‘Programmatic Supply Chain Transparency Study’ (ISBA & PWC, 2020)

<<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁵⁰³ Publishers 1 and 2.

⁵⁰⁴ Pidgeon D, ‘Where Did the Money Go? Guardian Buys Its Own Ad Inventory’ (*Mediatel: The Media Leader*, 6 October 2016) <<https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/>> accessed 24 May 2022.

⁵⁰⁵ Publisher 6.

⁵⁰⁶ Advertisers 3, 4 and 5.

4.2.2.2 Complexity and cost of intermediaries drives advertisers and publishers towards large platforms

Advertisers and publishers, particularly small ones, noted that cost and complexity issues associated with the use of intermediaries had pushed them towards using the services of large platforms. Two small publishers indicated that cost and simplicity were factors in their decision to rely on Google services instead of different intermediaries⁵⁰⁷, although another publisher complained that Google also charges a high fee for their services⁵⁰⁸. Two small advertisers further noted that they find it cheaper and easier to buy ads directly from Google and Meta instead of working with intermediaries to buy ads programmatically⁵⁰⁹. A large advertiser opined that this is likely a common occurrence with small advertisers⁵¹⁰. A 2019 survey of SME advertisers undertaken in the US seems to confirm the popularity of large platforms among SMEs. Of the SME digital advertisers it surveyed, 84% advertised through Facebook and 44% advertised through Google Ads⁵¹¹.

4.3 Other key issues identified by advertisers

Transparency in digital advertising was raised by many advertisers as a key challenge. As one advertiser put it, “the market is not transparent at all”⁵¹². Issues related to assessing the performance of digital advertising were mentioned the most frequently, but concerns were also raised about pricing and the use of data. Interviews suggested that this perceived lack of transparency has led to a lack of trust among advertisers, especially in relation to large platforms.

4.3.1 Independent auditing of measurement data

The majority of advertiser respondents said that they felt Google and Meta are not sufficiently transparent about the performance of their advertising services⁵¹³. Although these platforms do provide advertisers with some data about how their advertising campaigns perform, three advertisers said that they wanted to be able to independently audit and assess this data in order to verify its accuracy⁵¹⁴. As

⁵⁰⁷ Publishers 4 and 7.

⁵⁰⁸ Publisher 5.

⁵⁰⁹ Advertisers 3 and 9.

⁵¹⁰ Advertiser 1.

⁵¹¹ ‘2019 SBEC/TechnoMetrica Small Business Survey on Online Advertising’ (SBEC/TechnoMetrica, August 2019) <<https://sbecouncil.org/wp-content/uploads/2019/09/SBEC-Technometrica-Online-Advertising-Report-Sept-2019.pdf>>.

⁵¹² Advertiser 1.

⁵¹³ Advertisers 1, 2, 3, 4 and 6.

⁵¹⁴ Advertisers 1, 2 and 6.

one advertiser explained, “we can’t trust the data we get from platforms because it’s their data and most of the time it’s unaudited”⁵¹⁵. Finnish advertising association Marketing Finland said that advertisers feel like Google and Meta are not sufficiently transparent, which has contributed to a “lack of trust” in both companies (see 3.11 for more detail).

Advertisers claimed that large platforms impose various limits on using third-party ad verification and measurement to get an independent assessment. This is supported by industry surveys too. A 2020 survey of large advertisers undertaken by the World Federation of Advertisers (WFA) found that 79% said they encounter a lack of data sharing when working with large platforms, impacting their ability to “measure how many people saw an ad and whether a campaign on a particular platform was successful”⁵¹⁶. Nonetheless, the WFA survey’s sample covers a relatively small subset of large advertisers, and therefore may not be representative of how all advertisers feel, especially SMEs. One large advertiser explained that although some platforms have “conceded ground” to some extent when it comes to allowing third parties to perform measurement and verification on behalf of advertisers, there still is not sufficient visibility on the full range of metrics outlined above⁵¹⁷. As a result, one advertiser said they would like to see provisions introduced in EU law to make this mandatory for large platforms (e.g. the Digital Markets Act (DMA))⁵¹⁸.

This situation has led to a broader lack of trust in the relationship between advertisers and large platforms, leading some advertisers to draw conclusions that data is being deliberately withheld to conceal poor performance. One advertiser suggested that Meta restricts advertiser access to some data because advertising on the platform “doesn’t work”⁵¹⁹. An ongoing US class action lawsuit launched by a small advertiser in 2018 claims that metrics provided by Meta were inaccurate⁵²⁰. Two advertisers interviewed for this study said that they were uncertain that what consists as a “view” of an ad is sufficient, despite industry efforts to develop standard metrics around viewability⁵²¹. Additionally, several respondents said that

⁵¹⁵ Advertiser 2.

⁵¹⁶ ‘WFA Global Position on Advertiser Access to Data in the Digital Advertising Market’ (*World Federation of Advertisers*, 9 April 2021) <<https://wfanet.org/knowledge/item/2021/04/09/WFA-global-position-on-advertiser-access-to-data-in-the-digital-advertising-market>> accessed 8 June 2022.

⁵¹⁷ Advertiser 2.

⁵¹⁸ Advertiser 2.

⁵¹⁹ Advertiser 4.

⁵²⁰ Murphy H, ‘Facebook Reported Revenue It “Should Have Never Made”, Manager Claimed’ (*Financial Times*, 18 February 2021) <<https://www.ft.com/content/c144b3e0-a502-440b-8565-53a4ce5470a5>> accessed 2 June 2022.

⁵²¹ Advertisers 5 and 6.

they did not have access to enough information to be able to assess the effectiveness of ad targeting services provided by Google and Meta⁵²².

The DMA points out that the conditions under which gatekeepers provide digital advertising services to businesses, including both advertisers and publishers, “are often non-transparent and opaque” and that this “undermines their ability to switch between undertakings providing online advertising services”⁵²³. Article 6.8 DMA is designed to “further enhance fairness, transparency and contestability of online advertising services”⁵²⁴ by requiring gatekeepers to provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, with “access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data”⁵²⁵. Articles 5.9 and 5.10 DMA also require gatekeepers to provide information about pricing and fees to publishers and advertisers.

These measures could go some way to improving the availability of data for advertisers and publishers to make evidence-based decisions, but some industry experts interviewed for this study have pointed to possible limitations of these provisions that would need to be addressed in order to meaningfully improve transparency in the digital advertising ecosystem.

Firstly, some stakeholders argue that the DMA’s reference to “aggregated and non-aggregated” data is too broad. One representative of an advertiser association who has been involved in initiatives designed to improve transparency in the digital advertising industry suggested that advertisers need access to detailed “log-level” data in order to achieve effective transparency and enable the level of analysis needed to make evidence-based decisions about media investment.

⁵²² Advertisers 3, 4 and 6, Publisher 5.

⁵²³ Recital 45 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁵²⁴ Recital 58 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁵²⁵ Article 6.8 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

Secondly, it would also be important for all the data referenced in Articles 5.9, 5.10 and 6.8 DMA to be provided in a standardised format so that comparisons can be made across different platforms.

A bill introduced in the US Senate could help ensure that large platforms and intermediaries act in advertisers' and publishers' best interests, thereby improving trust⁵²⁶. The CTDA would place a "best interest duty" and a "best execution duty" on large platforms and intermediaries that generate more than \$5 million in digital advertising revenue. This would require SSPs and DSPs to "use reasonable diligence, care, and skill to act in the best interest" of their customers, not put their own interests ahead of their customers', and "seek the most favorable terms reasonably available under the circumstances for each order transaction" of their customers. The bill would also require owners of DSPs and SSPs to be transparent about the performance of their services.

4.3.2 Difficulties assessing measurement when advertising through publishers and intermediaries

Advertisers also reported that measuring the performance of their ads is "challenging" when working with publishers and intermediaries other than Google and Meta, largely because of a lack of standardisation across different platforms. As one advertiser noted, there is not "one standardised framework that works for all"⁵²⁷.

4.3.3 Pricing of advertising

Several respondents also said that they feel they do not have access to enough information about how Google sets the price of advertising. Two large advertisers complained that Google is not transparent about how it sets its prices and why they fluctuate, with one noting that they wished there was more transparency about Google's ad pricing algorithms⁵²⁸.

Qualitative research undertaken by Jigsaw Research on behalf of the CMA also found concerns about the pricing of large platforms' services among small advertisers in the UK⁵²⁹. It found that some small advertisers had a sense that both Google and Meta's bidding algorithms were changing constantly. This led

⁵²⁶ Competition and Transparency in Digital Advertising Act, SIL22678, 117th Cong. (2022) <<https://www.lee.senate.gov/services/files/7384B096-04C3-4A3A-9796-80D22483026F>>.

⁵²⁷ Advertisers 4 and 5.

⁵²⁸ Advertisers 1 and 3.

⁵²⁹ 'Digital Advertising Services Qualitative research report' (*Jigsaw Research and the Competition and Markets Authority*, June 2020) <https://assets.publishing.service.gov.uk/media/5efb3fded3bf7f769d2695af/Digital_Advertising_Services_Research.pdf>.

them to feel as though they had less control over their budget, with some small advertisers reportedly overspending unwillingly as a result. With Google, this issue was compounded by the fact that their contact with the platform was generally “very sales driven”. According to one small advertiser who spoke to Jigsaw Research, “I do give Google a budget, but they never seem to stick to it – ‘the higher the invoice, the more successful the campaign’ seems to be their approach”.

Publishers interviewed by the Australian Competition and Consumer Commission (the ACCC) similarly argued that lack of transparency in the pricing of Google Ads “allows Google to retain hidden amounts of advertiser expenditure”⁵³⁰. According to these publishers, “neither advertisers nor publishers can observe the outcomes of the relevant auctions or determine Google’s take rate for a particular ad impression”.

4.3.4 Poor customer service when working with large platforms

Three small advertisers said that their experience with large platforms’ customer service had often been unsatisfactory⁵³¹. Speaking about Google, one mentioned that they were “really hard to reach” and “slow to answer”⁵³², another mentioned that their customer service was “not useful”⁵³³. Speaking about Meta, one of these small advertisers opined that “the more you spend, the more help you get”⁵³⁴. One of these small advertisers noted that although large platforms’ services were generally user-friendly, “if you have questions about things that are not working, it’s hard to get things solved”, which they described as an “alienating experience”⁵³⁵. They described an example where their marketing manager had been “shut out” of their Facebook account during an important sales period and was unable to get a hold of a customer service representative to fix the issue for five days. They described the situation as “really frustrating”. A large advertiser also flagged during a workshop related to this study that one large platform has at times blocked their advertiser account for long periods without warning and without compensation.

⁵³⁰ ‘Digital Advertising Services Inquiry Final Report’ (Australian Competition and Consumer Authority, 2021), p. 153
<<https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf>>.

⁵³¹ Advertisers 3, 7 and 9.

⁵³² Advertiser 3.

⁵³³ Advertiser 7.

⁵³⁴ Advertiser 3.

⁵³⁵ Advertiser 9.

4.4 Other key issues identified by publishers

Publishers interviewed for this study all explained that they struggle to compete with large platforms for digital advertising revenue for a number of reasons related primarily to data but also reach and pricing. According to the Federation of European Data and Marketing (FEDMA), advertisers know that “it’s only through these huge platforms that they can reach the largest audiences”. Evidence collected based on interviews with advertisers supports this view, suggesting that advertisers allocate larger proportions of their advertising budgets to large platforms than to publishers. One large advertiser said that nearly half of their digital advertising spend went to large platforms and this had grown significantly over time⁵³⁶. Another advertiser said that they were spending “less and less” of their digital advertising budget with publishers, and increasingly with large platforms instead⁵³⁷. One large advertiser said “as much as we would like to have relationships and a diverse portfolio of publishers that we work with, sometimes we get distracted because these other ones [large platforms] are bigger, seem more powerful, have a louder voice and a greater number of sales teams”⁵³⁸. All of the small advertisers interviewed for this study said they spend at least 80% of their digital advertising budget with Google and Meta⁵³⁹, with two saying that these platforms account for 100% of their digital advertising spend⁵⁴⁰. None of the small advertisers interviewed said they advertise on publisher sites, with the exception of one B2B advertiser that bought a small amount of advertising directly from specialist media related to their product category⁵⁴¹. None of the small advertisers interviewed use programmatic advertising⁵⁴².

4.4.1 Access to data

Publishers generally said that data was an essential part of digital advertising for them because this is what advertisers expect, both for measurement and targeting⁵⁴³. However, interviewees said that some types of data are harder for publishers to obtain, creating a competitive disadvantage for them compared to large platforms. One large publisher noted that given that their main activity is producing content, they do not have the same “deepness of data”⁵⁴⁴. The European Publishers Council, which describes itself as a high-level group of

⁵³⁶ Advertiser 4.

⁵³⁷ Advertiser 5.

⁵³⁸ Advertiser 2.

⁵³⁹ Advertisers 3, 6 and 7.

⁵⁴⁰ Advertisers 6 and 7.

⁵⁴¹ Advertiser 3.

⁵⁴² Advertisers 3, 6 and 7.

⁵⁴³ Advertisers 1, 5, 6, and 7.

⁵⁴⁴ Publisher 1.

chairpersons and CEOs of publishers, said that large platforms can “collect and combine data into vast silos”. They suggested that “this is what advertisers love [...] and publishers can’t compete with that”. In particular, publishers noted the importance of, and their relative lack of access to, age, gender and socio-economic data⁵⁴⁵, intent data⁵⁴⁶, frequency data⁵⁴⁷, browsing data⁵⁴⁸ and search data⁵⁴⁹. Two publishers said that although they collected first-party data from their readers, they still needed to buy data from third-party vendors in order to attract advertisers⁵⁵⁰.

Furthermore, three publishers complained that they felt that EU regulation (in particular the General Data Protection Regulation (GDPR) and the ePrivacy Directive) is enforced more strictly on publishers than on large platforms⁵⁵¹, which puts them at a competitive disadvantage. This was also echoed by publisher association News Media Europe, which argued that people using Google do not always see “consent requests for being tracked for targeted ads”, but that this is the case when users visit publisher websites. This association also claimed that the GDPR provisions related to purpose limitation are not being enforced when it comes to large platforms and advertising data. According to News Media Europe, this allows platforms to “pull data from their entire ecosystems and develop advertising solutions that are just way out of [publishers’] reach”. One German publisher suggested that there was a much higher level of GDPR enforcement in Germany, particularly in relation to publishers and the collection of data for advertising purposes, compared to Google and Meta’s lead data protection supervisory authority in Ireland⁵⁵². Another publisher suggested that enforcement of the GDPR was fragmented (“GDPR is enforced in more ways than there are Member States”)⁵⁵³ creating legal uncertainty and meaning that different publishers are being held to different standards of compliance depending on where they are based. Some publishers said that they felt data protection regulation had increased their costs and reduced the amount of data they can collect⁵⁵⁴, while there was a perception that large platforms had been less impacted by the regulations and subsequent enforcement action.

Several publishers also raised concerns that shifts related to how the digital advertising industry collects data were likely to make it harder for them to

⁵⁴⁵ Publishers 1 and 2.

⁵⁴⁶ Publisher 1.

⁵⁴⁷ Publisher 2.

⁵⁴⁸ Publisher 3.

⁵⁴⁹ Publisher 5.

⁵⁵⁰ Publishers 1 and 2.

⁵⁵¹ Publishers 1, 6 and 8.

⁵⁵² Publisher 1.

⁵⁵³ Publisher 6.

⁵⁵⁴ Publishers 1 and 5.

compete with large platforms in the future. Some publishers argued that recent moves by Apple and Google to restrict third-party access to data (see section 1.3.1.2.2 and 5.2) were designed to give these companies more control over the digital advertising ecosystem, thereby reducing publishers' share of digital advertising spend⁵⁵⁵. One small publisher suggested that they felt Google would be "happy to pull the plug" on third-party access to data because it would make market participants "even more reliant on them"⁵⁵⁶, and two larger publishers said that they believed proposals being considered as part of Google's Privacy Sandbox initiative would likely increase publishers' and advertisers' reliance on Google⁵⁵⁷. Another publisher suggested that this could result in Google becoming a "key gatekeeper" for all new sources of personal data⁵⁵⁸. One small advertiser explained that they started buying advertising from Apple (Apple Search Ads) to promote their app after Apple introduced stricter opt-in requirements for ad tracking on mobile devices, leading them to conclude that Apple "made money out of the restrictions they introduced"⁵⁵⁹.

In response to these developments, most publisher respondents said that they had begun working to increase their store of first-party data, such as by developing larger logged-in ecosystems and premium content that they can monetise through subscriptions. Some have also started developing and improving technology to analyse content on their platforms in order to provide contextual targeting options to advertisers⁵⁶⁰. Publishers said that they hoped this would help them stay competitive, but also raised concerns that it could make the ecosystem more complex for advertisers to navigate by creating publisher "data silos" and fragmentation, making it more difficult to track the performance of campaigns across different publisher platforms⁵⁶¹.

It is important to note, however, that the interviews revealed that publishers vary quite widely in their approach to data: while some emphasised that they needed to increase their ability to collect all types of data in order to compete with large platforms for digital advertising revenue, others suggested that this was not essential. One publisher argued that interest data was not used for targeting as much anymore⁵⁶². Another noted that they had received feedback from their advertiser clients indicating that the use of "granular" targeting data and micro-targeting can actually have negative impacts on users' perceptions⁵⁶³. Two

⁵⁵⁵ Publishers 3, 5, 6 and 8; Advertiser 3.

⁵⁵⁶ Publisher 8.

⁵⁵⁷ Publishers 3 and 5.

⁵⁵⁸ Publisher 6.

⁵⁵⁹ Advertiser 3.

⁵⁶⁰ Publishers 1, 2, 3, 5 and 6.

⁵⁶¹ Publisher 1.

⁵⁶² Publisher 1.

⁵⁶³ Publisher 2.

publishers furthermore argued that expanding their user base and reach was a more sustainable way of increasing advertising revenues, as opposed to increasing monetisation through the collection of more personal data⁵⁶⁴.

4.4.2 Reach

Another area where publishers said they struggle to compete is the number of people that can be reached with a single ad (often termed "reach"). As outlined in section 4.1.1, reach is a motivating factor for advertisers to buy digital advertising. Concentrating ad spend in one platform that a lot of people use can generate efficiencies for advertisers. Most European publishers are not able to compete with large platforms in terms of reach. BILD.de, one of the leading news portals in Germany, had on average 26.5 million unique users per month on average in 2021⁵⁶⁵. In comparison, during the same period, Facebook.com had over 43 million users per month on average in Germany⁵⁶⁶, and 2.8 billion globally⁵⁶⁷.

Programmatic advertising (see section 1.3.1) has evolved to provide advertisers with a way of getting reach across multiple publisher sites through a common system. To some extent this enables publishers to access advertising revenue from advertisers who otherwise would not consider them due to their relatively small reach compared to large platforms. One large advertiser described programmatic as "healthier for the ecosystem so smaller publishers get more ad spend"⁵⁶⁸. This means that programmatic advertising is seen as essential by many publishers. "If we shut down programmatic tomorrow, then the ad revenue would just go elsewhere and then we wouldn't be able to fund our journalism" said one large publisher⁵⁶⁹. However, as outlined above, working with intermediaries that provide programmatic advertising services is often seen as expensive and complex for both publishers and advertisers. In addition, large platforms (especially Google) hold leading market positions in many parts of the programmatic intermediary ecosystem, which raises a number of challenges for publishers (see section 4.2.1).

⁵⁶⁴ Publishers 2 and 8.

⁵⁶⁵ 'Bild Digital - Nothing Moves Germany Like Bild - The Biggest Entertainment & News Portal!' (*Media Impact*) <<https://www.mediaimpact.de/en/portfolio/bild-digital-2>> accessed 12 July 2022.

⁵⁶⁶ 'Germany Monthly Number of Facebook Users 2022' (*Statista*)

<<https://www.statista.com/statistics/1017402/facebook-users-germany/>> accessed 12 July 2022.

⁵⁶⁷ 'Facebook, Inc. Form 10-K for the Fiscal Year Ended December 31, 2020' (2020)

<<https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf>>.

⁵⁶⁸ Advertiser 4.

⁵⁶⁹ Publisher 6.

Some publishers develop direct relationships with a number of advertisers, agreeing “direct deals” where a fixed amount of advertising is negotiated directly between the publisher and the advertiser. Sometimes these direct deals are delivered using parts of the programmatic advertising infrastructure (known as “programmatic direct”) or they can be delivered outside of this system (“direct”). However, these types of deals require additional resources on the publisher and advertiser side. One publisher explained that direct deals can be difficult to scale because of how long they take to secure⁵⁷⁰ and an advertiser said that securing and measuring the performance of direct deals can be “very time consuming”, especially when working with multiple different publishers⁵⁷¹. In addition, direct deals with smaller publishers can be less attractive for large advertisers, due to their small reach⁵⁷².

The French competition authority, *Autorité de protection des données (ADLC)*, found that direct deals typically account for 30-75% of the advertising revenue of “major publishers”⁵⁷³. It found that direct deals could be more valuable for publishers than selling advertising space programmatically, with local publishers *Le Figaro* and *Webedia* stating that they were able to generate 30-60% higher revenues. However, other publishers interviewed as part of this study explained that although direct deals can provide better margins and control than selling through auctions, the volume of sales will generally be smaller⁵⁷⁴. Furthermore, as the ADLC notes, “direct sales are generally priced higher than programmatic sales, particularly as they typically involve the most attractive inventory”⁵⁷⁵. This highlights that the value that publishers that derive from direct deals can vary based on the attractiveness of their inventory (which can depend on e.g. the size of their readership, the content they produce and their reputation).

4.4.3 Pricing

One large publisher explained that their limitations in relation to data and reach contribute to raising their costs and therefore the price of advertising on their platforms. They argue that this puts them at a competitive disadvantage. The

⁵⁷⁰ Publisher 1.

⁵⁷¹ Advertiser 4.

⁵⁷² Advertiser 1.

⁵⁷³ ‘Decision 21-D-11 of June 07, 2021 Regarding Practices Implemented in the Online Advertising Sector’ (*Autorité de la Concurrence*, 2021), p. 14 <<https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-online-advertising-sector>>.

⁵⁷⁴ Publishers 3 and 5.

⁵⁷⁵ ‘Decision 21-D-11 of June 07, 2021 Regarding Practices Implemented in the Online Advertising Sector’ (*Autorité de la Concurrence*, 2021), p. 14 <<https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-online-advertising-sector>>.

publisher said that they need to price in additional costs of acquiring third-party data, as well as the “efforts and investments” they make to ensure first-party data is collected lawfully (see also 4.4.1). The publisher argued that, because of their size, large platforms are conversely in a position to provide ad targeting “for free” to advertisers⁵⁷⁶. The publisher explained that this made it impossible for them to compete with large platforms on price.

⁵⁷⁶ Publisher 1.

4.5 Conclusion

Advertisers consider that one of the key benefits of digital advertising is the ability to reach large audiences and target groups of people who are likely to be interested in what they are advertising. They also appreciate the ability to gain insights on the effectiveness of their digital advertising campaigns using measurement data. Advertisers estimate that digital advertising is a cost-effective way of reaching their target audiences.

There is a perception that the value of digital advertising is higher when it can be targeted based on detailed knowledge about the individual who is likely to view the ad (usually linked to profiling based on personal data). However, there appears to be limited empirical evidence to support this notion.

Both advertisers and publishers described negative experiences when dealing with large platforms. They complained of feeling dependent on large platforms and expressed that they would like the digital advertising ecosystem to offer more alternative options. Publishers said that they expected to lose revenue if they stopped working with Google. Publishers and advertisers also expressed concerns that moves by Google and Apple to restrict third-party tracking could lead to less transparency and less competition in digital advertising.

Both advertisers and publishers noted that working with intermediaries involved high costs and often lacked transparency, but it is nonetheless essential for publishers to do so. Small advertisers and publishers both noted that the costs and complexity associated with the use of intermediaries contributed to their decision to work with large platforms instead.

Advertisers are highly reliant on data to measure the performance of ads, but say they have difficulty accessing it, especially when working with Google and Meta. This had led to a lack of trust. Several advertisers also feel that they do not have enough information about how Google sets its prices.

Publishers described Google and Meta as their most important competitors, as they are often perceived by advertisers as simpler and sometimes cheaper options for digital advertising. Publishers explained that they struggle to compete with large platforms for reasons primarily related to data, reach and pricing. Platforms are seen as an easy way for advertisers to reach large numbers of potential customers.

4.6 Interview methodology

Respondents were based in various European Economic Area (EEA) countries, including Germany, the Netherlands, Belgium, Austria, Sweden, Czechia, Norway, France and Denmark. See table 7 for an overview of the advertisers and publishers interviewed for the study.

Interview questions for advertisers and publishers were designed to solicit open, spontaneous responses, which were analysed to identify common themes and patterns in relation to different groups of stakeholders. The interviews with publishers and advertisers were supplemented with interviews with relevant trade associations representing advertisers, publishers and intermediaries. In the analysis, relevant evidence collected through desk research was considered in relation to respondents' statements, where relevant.

Respondents were given the option to speak on an anonymous basis so as to be able to gather as much honest and "unfiltered" feedback as possible. Additionally, respondents' interests and incentives were taken into account when writing this section, and certain statements were checked against the relevant evidence, so that facts could be more easily differentiated from respondents' personal opinions.

Interviewee label	Interviewee
Advertiser 1	Norman Wagner, Head of Group Media, Deutsche Telekom
Advertiser 2	Anonymous
Advertiser 3	Anonymous
Advertiser 4	Anonymous
Advertiser 5	Anonymous
Advertiser 6	Romain Felix, Co-Founder, WoodCutter
Advertiser 7	Célia Maublanc, Digital Marketing Manager, Hue Dada
Advertiser 8	Anonymous
Advertiser 9	Sune Blicher, Head of Communications, CPH Film Festivals
Publisher 1	Anonymous
Publisher 2	Anonymous
Publisher 3	Anonymous
Publisher 4	Libor Matoušek, CEO, Drbna
Publisher 5	Anonymous
Publisher 6	Dorthe Bjerregaard-Knudsen, Executive VP, COO, and Thomas Lue Lytzen, Director of Ad Sales & Tech, JP/Politikens Hus
Publisher 7	Anonymous
Publisher 8	Anonymous

Table 7: advertisers and publishers interviewed for part B.

Part C

What would a more transparent, balanced and sustainable digital advertising ecosystem look like?

5 Alternative digital advertising models

Although the most widely used forms of digital advertising today rely on large amounts of personal data and profiling of individuals, less intrusive alternative models are emerging. Some of these models could have a positive privacy impact, although not all of them would limit the systematic monitoring and profiling of individuals. More independent data about the performance of these models compared to the status quo is needed to encourage widespread adoption among advertisers and publishers.

This section will consider two alternative digital advertising models which are currently in use in the market or in development. It will also consider other emerging digital advertising tools and subscriptions, which are an important alternative method of revenue generation for publishers.

As described in section 1, personal data (including special category data)⁵⁷⁷ plays an essential role in targeting ads and measuring the performance of advertising campaigns today. These activities are often tied to unique identifiers that enable companies to build up a picture of an individual's behaviour across sites, apps, platforms and devices. The sharing of personal data with multiple third parties is often an inherent part of the current digital advertising model, although this is changing as large platforms like Google introduce restrictions on third-party tracking (see section 1.3.1.2 and 5.2).

In the current digital advertising ecosystem, buying and selling ads without the use of personal data is rare. As outlined in section 4, advertisers and publishers say that a key benefit of digital advertising is the ability to use data to target ads towards people who are likely to be interested in their products and services and measure their performance⁵⁷⁸. However, as section 2.4 concluded, there is limited data available to assess and compare different types of targeting and, most importantly, different approaches to the use of personal data in relation to advertising bought directly from large platforms, even though these channels make up a significant part of digital advertising. As a result, most advertisers default to the most common methods of buying advertising, which all tend to

⁵⁷⁷ See section 1.3.2.

⁵⁷⁸ Advertisers 1, 3 and 4.

involve (a) the monitoring of individual behaviour and the profiling of individuals (b) the processing of special categories of data, as defined by Article 9 General Data Protection Regulation (GDPR) (also referred to as “sensitive personal data”) (c) the sharing of personal data with multiple third parties. As discussed in section 2, these characteristics, which are an inherent part of today’s digital advertising ecosystem, can have a negative impact on privacy, data protection, democracy and society, and the environment.

However, digital advertising models exist that offer an alternative to the status quo. These models, which are summarised and analysed in this section, claim to use less (or no) personal data and, as a result, may involve less monitoring and profiling of individuals and/or less data sharing with third parties. In the wake of moves by Google and Apple to restrict third-party tracking within their ecosystems (Chrome, Android and iOS), advertisers and publishers are showing increasing interest in some of these models as a way to mitigate the anticipated negative impacts of reducing tracking and third-party data sharing in a digital advertising context.

In this section, a selection of these “alternative” digital advertising models will be evaluated according to the following criteria:

- **Monitoring and profiling:** does the model rely on the monitoring of individual behaviour and the profiling of individuals?
- **Use of sensitive data:** does the model involve the processing of special categories of data (according to Article 9 GDPR)⁵⁷⁹?
- **Third-party data sharing:** does the model involve the sharing of personal data with multiple third parties (such as digital advertising intermediaries)⁵⁸⁰?

Our research has indicated that, today, some of the models evaluated in this section are often used in combination with additional targeting and measurement which would not meet the criteria above. Therefore, this evaluation assumes that each model is used on its own, rather than in combination with the current digital advertising model. For example, we evaluate a version of contextual advertising that would not involve the use of any personal data (or persistent identifiers), and

⁵⁷⁹ As discussed in section 1.3.2, the use of demographic, interest, intent and location data could all involve the use of special category data, which the GDPR defines as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.” *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1, <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

⁵⁸⁰ See section 1.2.2.4.

we assume that local profiling models do not use data collected by third parties. This will be explored in further detail in each section below.

Table 8 presents an overview of this section’s findings. All the models evaluated could reduce, to some extent, at least one of the three criteria outlined above. However, while local profiling models (such as the proposals being developed under Google’s Privacy Sandbox) may reduce the sharing of data among third parties in the digital advertising ecosystem, these models would mostly still rely on the monitoring and profiling of individuals by at least one company acting in a gatekeeper role.

This section will briefly describe each model with a specific focus on these three criteria. The impact of each model on publishers and advertisers will be evaluated according to the issues respondents described in section 4, and barriers to (or incentives for) adoption will be considered. This section’s findings will be considered in relation to the current regulatory framework (e.g. the GDPR) and proposed instruments (e.g. the Digital Services Act (DSA)⁵⁸¹ and the Digital Markets Act (DMA))⁵⁸².

	Monitoring and profiling?	Use of sensitive data?	Third-party data sharing?
Current digital advertising model	✓	✓	✓
Contextual advertising	✗	✗	✗
Local profiling	✓	✓	✗
Subscriptions	✗	✗	✗

Table 8: Overview of whether each model relies on monitoring and profiling, involves the use of sensitive data, or involves the sharing of personal data with multiple third parties.

⁵⁸¹ 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁵⁸² 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

This section was drafted using evidence collected through interviews undertaken between January and April 2022 with nine advertisers and eight publishers, including five small- and medium-sized enterprise (SME) advertisers and three SME publishers. Interviews were also conducted with providers and developers of alternative digital advertising models, relevant trade associations and industry experts. Relevant case studies on the effectiveness of alternative digital advertising models were analysed, and desk research was carried out. See table 7 in section 4.6 for an overview of the advertisers and publishers interviewed for the study.

5.1 Contextual advertising

Contextual advertising can reduce the privacy impact of digital advertising by targeting ads based on content rather than information tied to a specific individual. The privacy benefits of contextual advertising can be limited, though, if contextual data is used as a proxy for (sometimes sensitive) personal data and tied to individual identifiers that enable people to be profiled and monitored based on the content they view. More independent data about the performance of contextual advertising compared to the status quo is needed to encourage widespread adoption among advertisers and publishers.

There are many different interpretations of the term “contextual advertising”. It is sometimes understood to mean digital advertising that is targeted based on the content being viewed without using personal data about the person viewing it. However, in practice, methods that are described as “contextual advertising” today often do involve the processing of personal data. This is discussed further in section 5.1.3.

Although in its most basic form, contextual advertising can provide ad targeting options based purely on the content being viewed, the context itself can be recorded and used as a proxy for different types of data including interest data, intent data and demographic data (see sections 1.3.2 and 2.2.2). The use of context in this way may involve processing of personal data in such a way to trigger the application of the GDPR. Many current contextual models also process personal data in order to measure performance metrics, such as how many times a single user viewed an ad.

Given that there appears to be no standard industry definition of “contextual advertising” that explicitly excludes the use of personal data and/or persistent identifiers, it is important to note that simply describing a method as “contextual” does not necessarily imply less (or no) monitoring or profiling of individuals. Our evaluation below aims to focus on contextual advertising practices that do not use

personal data or persistent identifiers. Our assessment and resulting conclusions should not be applied to other models which are described as “contextual” but nonetheless rely on personal data for targeting, monitoring and profiling.

In practice, contextual advertising relies on being able to target ads based on the content being viewed (e.g. articles and videos). This is most commonly done in two ways: (1) analysis of the content being viewed, for example by identifying and analysing the presence of specific keywords, and (2) analysis of the URL of a webpage.

5.1.1 Contextual advertising based on keywords and textual analysis

The most typical form of contextual advertising might see an advertiser target ads at users viewing websites containing relevant keywords. For example, a package holiday provider might target keywords associated with its destinations (e.g. “Spain” and “summer”). This form of contextual advertising is provided by companies in the EEA such as Kobler (Norway), Opt Out Advertising (Netherlands) and Qwarry (France). Keyword-based contextual advertising is also the basis of search advertising⁵⁸³, although while solutions such as DuckDuckGo⁵⁸⁴ and Qwant⁵⁸⁵ claim to deliver search ads solely on a contextual basis, Google Search ads are typically used in combination with targeting based on profiling⁵⁸⁶.

A downside to keyword-based targeting is that it could inadvertently target irrelevant articles, for example a sport blog referring to football clubs in “Spain” during the “summer” transfer window. Consequently, contextual advertising systems increasingly use natural language processing (NLP) to gain a better understanding of the meaning of a webpage through techniques such as grammatical analysis and analysis of the sentiment, opinion and emotions of the content in question⁵⁸⁷. NLP can also be used by some advertisers as a brand safety tool because it enables the identification of content that they do not want their ad to appear next to and prevents ads from being served there (see section 5.1.3.5).

⁵⁸³ See section 1.1.2.1.

⁵⁸⁴ ‘Advertising and Affiliates’ (*DuckDuckGo*), <<https://help.duckduckgo.com/duckduckgo-help-pages/company/advertising-and-affiliates/>> accessed 7 June 2022.

⁵⁸⁵ ‘Qwant Advertising’ (*Qwant*), <<https://about.qwant.com/en/advertising/>> accessed 7 June 2022.

⁵⁸⁶ ‘Create a Search Campaign’ (*Google*). <<https://support.google.com/google-ads/answer/9510373>> accessed 2 June 2022.

⁵⁸⁷ See for example: Flood V, ‘The Tech Sessions: How Semantic Contextual Targeting Works’ (*VideoWeek*, 16 January 2017) <<https://videoweek.com/2017/01/16/the-tech-sessions-how-semantic-contextual-targeting-works/>> accessed 17 May 2022; Dai Z and others, ‘Transformer-XL: Attentive Language Models Beyond a Fixed-Length Context’ (*arXiv*, 2 June 2019) <<http://arxiv.org/abs/1901.02860>> accessed 17 May 2022; ‘Product’ (*Peer39*) <<https://www.peer39.com/product>>.

5.1.2 Contextual advertising based on URL embeddings

URL embedding models analyse the URL of the page where an ad will appear (e.g. <<https://www.irishtimes.com/life-and-style/health-family/parenting>>) to enable relevant targeting. These models use NLP to predict the likelihood that an ad will lead a user to take a desired action (e.g. buy a product). US company Dstillery⁵⁸⁸ and UK company Jellyfish⁵⁸⁹ are two providers of digital advertising based on URL embeddings. Both started providing these models in 2018. Their models follow a reasoning similar to contextual advertising, whereby a user visiting a website for a particular type of content is likely to be interested in ads that are relevant to that content. For example, “a user on shoe websites may be shopping for shoes, and a user reading about sports may be interested in tickets or ways to live stream games”⁵⁹⁰. In some cases, URL embeddings can be combined with keywords and textual analysis (see above). According to Dstillery, “keyword data extracted in the traditional contextual approach can be used as an enhancement”⁵⁹¹.

Although the application of URL embeddings in digital advertising can take place without the use of identifiers, as the technology stands, personal data appears to be necessary to train the underlying models. Both Dstillery and Jellyfish note in white papers that the models they use were trained using personal data⁵⁹², including data collected through real-time bidding (RTB). Currently, Dstillery’s solution uses a panel of 100,000 users per market to train its model⁵⁹³. This data is used by Dstillery strictly to train the model, rather than to target ads at the individuals who make up the panel.

⁵⁸⁸ White A and others, ‘Privacy-Friendly ID-Free Digital Ad Targeting Using URL Embeddings’, (*IEEE International Conference on Big Data*, 2020) <https://dstillery.com/wp-content/uploads/2021/05/2020-IDFree_IEEE_BigData.pdf> accessed 18 May 2022.

⁵⁸⁹ Qiu Y and others, ‘Predicting Conversions in Display Advertising Based on URL Embeddings’ (*arXiv*, 28 August 2020) <<http://arxiv.org/abs/2008.12003>> accessed 18 May 2022.

⁵⁹⁰ White A and others, ‘Privacy-Friendly ID-Free Digital Ad Targeting Using URL Embeddings’, (*IEEE International Conference on Big Data*, 2020), p. 1721 <https://dstillery.com/wp-content/uploads/2021/05/2020-IDFree_IEEE_BigData.pdf>, accessed 18 May 2022.

⁵⁹¹ White A and others, ‘Privacy-Friendly ID-Free Digital Ad Targeting Using URL Embeddings’, (*IEEE International Conference on Big Data*, 2020), p. 1721 <https://dstillery.com/wp-content/uploads/2021/05/2020-IDFree_IEEE_BigData.pdf> accessed 18 May 2022.

⁵⁹² White A and others, ‘Privacy-Friendly ID-Free Digital Ad Targeting Using URL Embeddings’, (*IEEE International Conference on Big Data*, 2020) <https://dstillery.com/wp-content/uploads/2021/05/2020-IDFree_IEEE_BigData.pdf> p.1722, accessed 18 May 2022; Qiu Y and others, ‘Predicting Conversions in Display Advertising Based on URL Embeddings’ (*arXiv*, 28 August 2020), p. 4 <<http://arxiv.org/abs/2008.12003>> accessed 18 May 2022.

⁵⁹³ The individuals on the panel in question have consented to having their online behaviour tracked on a continuous basis by a third-party data broker.

5.1.3 Evaluation

5.1.3.1 Use of personal data

Some contextual advertising vendors use contextual information as just one signal among many to target ads. Other signals can include personal data gathered by third parties and information from advertising profiles linked to ad identifiers. In some cases, contextual information can be used to infer personal data and profile individuals by linking to persistent identifiers that collate multiple sources of data. For example, Google’s current “contextual targeting” solutions are supplemented by “language and location targeting, a visitor’s recent browsing history and other factors”⁵⁹⁴. Our research suggests that contextual advertising that connects contextual information to a persistent advertising identifier can be used to replicate many of the data practices which are common under the current digital advertising model: contextual information can be “converted” into interest data, intent data or even demographic data through the use of inferences and profiling. This can include data that would be considered as special category data under Article 9 GDPR. If this information is fed into auctions based on personal data (e.g. RTB) it can be shared with multiple third parties.

This nuance is important from a policy perspective. Discussions of digital advertising in the context of the DSA, for example, have sometimes assumed that contextual advertising never involves the use of personal data. In their opinion on the DSA, the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs called for the legislation to phase out “behavioural and personalised targeting” and “be replaced by contextual advertising”, on the assumption that “displaying contextual advertisements does not require processing personal data and is thus less intrusive”⁵⁹⁵. Future policy discussions that look to incentivise the use of contextual advertising that does not use personal data should consider how to ensure that the language used, especially around definitions, is precise enough to signal a clear distinction.

The following evaluation is based on contextual advertising that does not use personal data. The assessment and resulting conclusions should not be applied to other models that are described as “contextual” but nonetheless rely on personal data for targeting, monitoring and profiling.

⁵⁹⁴ ‘Contextual Targeting’ (*Google Ads Help*) <<https://support.google.com/google-ads/answer/1726458?hl=en>> accessed 8 May 2022.

⁵⁹⁵ Breyer P, ‘Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC (COM(2020)0825 – C9- 0418/2020 – 2020/0361(COD))’ (*European Parliament Committee on Civil Liberties, Justice and Home Affairs*, 2021) <https://www.europarl.europa.eu/doceo/document/LIBE-AD-692898_EN.pdf> Amendment 11.

5.1.3.1.1 Monitoring and profiling

Contextual advertising that does not link contextual information to persistent ad identifiers cannot, in theory, be used to monitor and profile individuals. Removing identifiers from the model means that profiles cannot be built up over time: an ad is served based on the content an individual is viewing at that particular moment.

5.1.3.1.2 Sensitive data

Contextual information can be used as a proxy to infer interest data, intent data and demographic data. In some cases, such data could reveal special category data under Article 9 GDPR, such as political opinions, religious beliefs, racial or ethnic origin, health data or data about a person's sex life or sexual orientation. This means that contextual information can be used to target ads based on inferred special category data. Even if targeting segments are not explicitly linked to special category data, ads could still be targeted based on inferences linked to context, for example if an advertiser chooses to target ads based on contexts that include the keywords "gay" and "lesbian". This could lead to the perpetuation of harmful stereotypes and, in some cases, discrimination. As outlined in section 2.2.2, studies have shown that non-sensitive attributes can be used to target advertising in discriminatory ways⁵⁹⁶.

The DSA introduces a prohibition on providers of online platforms to present on their interfaces advertising "based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679"⁵⁹⁷. However, some civil society stakeholders consulted for this study expressed concern that the wording of Article 26.3 DSA was not sufficiently precise to prohibit non-special category data from being combined and inferred to create new targeting options which could be considered sensitive, for example targeting individuals based on an interest in certain topics known to be linked to (albeit not explicitly), or be proxies for, areas such as sexual orientation, religion or health.

⁵⁹⁶ For example, Speicher et al. found that large numbers of non-sensitive attributes for targeting ads on Facebook seemed to correlate with protected characteristics under equality law and could be used to create highly discriminatory ad targeting. Speicher T and others, 'Potential for Discrimination in Online Targeted Advertising' in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR, 2018) <<https://proceedings.mlr.press/v81/speicher18a.html>>.

⁵⁹⁷ Article 26.3 of the Digital Services Act. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

5.1.3.1.3 Third-party data sharing

Where contextual advertising is bought and sold using programmatic technology (see section 1.2.2.4), some contextual information can be shared with third parties in bid requests. As outlined above, some of this information could be used to infer characteristics about the individual to whom the ad will be served and, if linked to a persistent identifier, could be used to build advertising profiles over time. Interviews with several contextual advertising vendors indicated that it is possible to sell and deliver contextual ads without using any personal data, including persistent identifiers. They claim, furthermore, that without the use of persistent identifiers, the advertisers or intermediaries that deliver the contextual ad cannot identify the user to whom it was shown. This could significantly reduce the amount of personal data shared with third parties compared with the current digital advertising model.

5.1.3.2 Limited independent evidence to assess the effectiveness of contextual advertising

There is limited independent data available concerning the effectiveness of contextual advertising compared to the effectiveness of the current digital advertising model. The studies that do exist primarily take the form of small-scale surveys and case studies and are often developed by vendors of contextual advertising solutions and other intermediaries. This section will offer an overview of the available data and an assessment of some of the limitations and areas for further research.

Several advertisers indicated during interviews that they have launched their own research into the effectiveness of contextual advertising, but the outputs and details of these studies have not been shared with us. One large advertiser said that initial tests they had run showed that they could get “the same results” from contextual targeting compared to “super hyper targeting”⁵⁹⁸. Another said they believe that “contextual advertising is going to be just as effective as very specific audience targeting”⁵⁹⁹.

Several vendors of contextual advertising solutions have developed case studies on successful campaigns which used the technologies they sell. A campaign in the Netherlands that used Opt Out Advertising’s contextual advertising solution reported click-through rates that were 6% higher than ad networks using the current digital advertising model⁶⁰⁰ and conversions rates that were 15%

⁵⁹⁸ Advertiser 1.

⁵⁹⁹ Advertiser 4.

⁶⁰⁰ Misra S, ‘What is Contextual Advertising? How Does it Work?’ (*AdPushUp*, 18 June 2021) <<https://www.adpushup.com/blog/what-is-contextual-advertising-how-does-it-work/>>.

higher⁶⁰¹. Rev·Amp, another contextual advertising vendor, claims that contextual click-through rates can be three times higher than ads targeted under the current digital advertising model, although the methodology and data to support this claim has not been published⁶⁰². Dstillery has published case studies⁶⁰³ which indicate a positive impact on overall sales for companies using their contextual advertising tools, but they do not include detailed comparative information such as click-through rates or other attention metrics.

A quantitative study of video ads on YouTube undertaken by IPG Media Lab and brand safety vendor Zefr (which sells technology solutions enabling ads to be targeted based on context) found that ads delivered via contextual targeting (i.e. based on the content of a video) performed better than digital advertising based on profiling⁶⁰⁴. It found that the purchase intent of users who were shown contextually relevant ads was 63% higher than for users shown ads based on profiling, and that these users were 83% more likely to recommend the product in the ad and 40% more positive about the brand ("brand favourability"). A separate study of contextually delivered ads on YouTube by the University of South California in partnership with brand safety vendor Channel Factory similarly found that contextual ads were 93% more memorable than contextually "misaligned" ads⁶⁰⁵. These studies indicate that targeting ads based on context can have a positive impact from an advertiser perspective, although it is not clear whether contextual advertising that does not use persistent identifiers was tested. In addition, neither of these studies is independent: both were carried out by intermediaries which sell ad tech solutions that enable ads to be targeted based on context.

Various consumer surveys carried out by advertising intermediaries have suggested that placing ads in a relevant context can have a positive impact on brands, although these studies do not look at contextual targeting specifically. In a 2020 DoubleVerify survey, 69% of respondents said that they were more likely

⁶⁰¹ 'Pink Marketing achieves a 15% conversion increase in online campaign for AD and the regional publications' (*Opt Out Advertising*, 27 January 2022)

<<https://optoutadvertising.com/en/cases/algemeen-dagblad-en/>>.

⁶⁰² Hemsworth F, 'Contextual Advertising For Publishers: Skyrocket Your Revenue' (*RevAmp*, 3 March 2022) <<https://revamp.softonic.com/blog/contextual-advertising-for-publishers-skyrocket-your-revenue/>>.

⁶⁰³ See for example: 'ID-free Custom AI Audiences Grow Shipment Bookings for Logistics Company' (*Dstillery*) <<https://dstillery.com/success-stories/logistics-id-free-custom-ai-case-study/>> and 'ID-free Custom AI Delivers Paw-some Results for Pet Supply Brand' (*Dstillery*) <<https://dstillery.com/success-stories/pet-supply-id-free-custom-ai-case-study/>>.

⁶⁰⁴ 'New Study Reveals More Effective Way for Brands to Connect with Consumers' (*Business Wire*, 16 March 2016) <<https://www.businesswire.com/news/home/20160316005448/en/New-Study-Reveals-Effective-Brands-Connect-Consumers>>.

⁶⁰⁵ 'Contextually Aligned Ads Drive a 93% Increase in Brand Awareness, USC and Channel Factory Find' (*ExchangeWire*, 20 May 2020) <<https://www.exchangewire.com/blog/2020/05/20/contextually-aligned-ads-drive-a-93-increase-in-brand-awareness-usc-and-channel-factory-find/>>.

to look at an ad that is contextually relevant⁶⁰⁶ and a MetrixLab survey found that placing ads next to “relevant” content can increase individuals’ positive feelings about a brand by 6-22%⁶⁰⁷. However, these surveys offer a limited view into the effectiveness of contextual targeting compared to ads that are targeted based on profiling. Also, they are not independent: both surveys were carried out by firms that sell ad tracking and measurement technologies, and DoubleVerify is a contextual advertising provider.

More independent research on the effectiveness of contextual advertising compared to ads based on profiling is needed to draw conclusions about the viability of this type of advertising, especially from an advertiser perspective. This type of evidence could help advertisers predict the potential impact of adopting contextual advertising models in favour of the model they currently use and manage any associated risk. Some of the biggest advertisers interviewed for this study indicated that they are investing significant resources in carrying out this type of research internally, but this is out of the reach of most small advertisers.

5.1.3.3 Limited options for targeting but technology is improving as advertiser expectations are decreasing

Advertisers and publishers interviewed for this study said that a key benefit of digital advertising is the ability to use data to target ads towards people who are likely to be interested in their products and services⁶⁰⁸. Contextual advertising was seen by some as a “less granular”⁶⁰⁹ method of targeting ads to individuals compared to the current digital advertising model based on personal data, monitoring and profiling. Small advertisers in particular see this as a risk⁶¹⁰, because “we lose money if we show ads to people who are not interested”⁶¹¹. At the same time, several large advertisers emphasised that they do not require “granular targeting”⁶¹² for their digital advertising campaigns. One large advertiser said that more and more often they “get rid of targeting”⁶¹³ based on personal data, while another said they no longer use ads based on profiling because they “do not want to chase people across the internet”⁶¹⁴. As one large advertiser put it, “The focus a long time ago was on audiences and context – I would want to

⁶⁰⁶ ‘Four Fundamental Shifts in Media & Advertising During 2020’ (*DoubleVerify*, 23 September 2020) <<https://doubleverify.com/four-fundamental-shifts-in-media-and-advertising-during-2020/>>.

⁶⁰⁷ ‘Efficiently reach users through visual media’ (*MetrixLab*, 2021)

<<https://www.metrixlab.com/whitepaper-efficiently-reach-users-through-visual-media/>>.

⁶⁰⁸ Advertisers 1, 3 and 4.

⁶⁰⁹ Advertiser 5.

⁶¹⁰ Advertisers 3, 6 and 7.

⁶¹¹ Advertiser 6.

⁶¹² Advertisers 1, 2 and 5.

⁶¹³ Advertiser 1.

⁶¹⁴ Advertiser 5.

advertise on [a premium publisher site] because of the environment. The pendulum has swung wildly over the last 20 years to the point where it is just all about the audience. If we could bring context back into the conversation by stopping the rapacious collection, storage and usage of data, then you would have to rely more on context”⁶¹⁵.

Many stakeholders interviewed for this study also indicated that the technology used for contextual advertising is evolving, and predictions of users’ characteristics are increasingly being used as proxies for their personal data. For example, a Global Head of Media Management at a large advertiser said that contextual advertising was likely to “work even better than it did 15 years ago because we can use advanced algorithms that can really see what is in an article or a video; in the past, it was hit and miss”⁶¹⁶. Indeed, contextual targeting can today be used to target ads by predicting demographic data, for example the age and gender of the user viewing the content. COO and co-founder of Qwarry Julie Walther indicated that Qwarry’s solutions are able to do this based on panel data collected and processed outside of ad delivery. Similarly, URL embedding models can use panel-based training to predict the likely location and time of day of users opening specific URLs, and target ads accordingly⁶¹⁷. This seems to indicate that predictive models could soon be able to predict additional characteristics of users based on increasingly sophisticated analysis of context.

5.1.3.4 Limited ability to measure the effectiveness of campaigns

Advertisers’ ability to measure the effectiveness of individual campaigns is limited when using contextual advertising, including URL embeddings. According to the contextual advertising providers interviewed as part of this study (Kobler, Opt Out Advertising, Qwarry and Dstillery), while it is possible to count impressions, clicks and viewability in real time through contextual advertising, without the use of identifiers, it is not possible to measure reach, frequency and conversions^{618, 619}. They explained that this is because impressions, clicks and views can be reported by the browser back to the intermediary involved in the contextual campaign without the use of an identifier. Reach, frequency and conversions, on the other hand, all typically require an identifier. For example, in the case of conversions,

⁶¹⁵ Advertiser 1.

⁶¹⁶ Advertiser 4.

⁶¹⁷ White A and others, ‘Privacy-Friendly ID-Free Digital Ad Targeting Using URL Embeddings’, (*IEEE International Conference on Big Data*, 2020), p. 1723 <<https://dstillery.com/wp-content/uploads/2021/05/2020-IDFree-IEEE-BigData.pdf>> accessed 18 May 2022.

⁶¹⁸ See also: Sluis S, ‘The Crawl, Walk, Run Guide To Contextual Targeting’ (*AdExchanger*, 10 February 2021) <<https://www.adexchanger.com/online-advertising/the-crawl-walk-run-guide-to-contextual-targeting/>> and ‘Understanding contextual targeting’ (*IAB UK*, 24 August 2021) <<https://www.iabuk.com/user-identity/understanding-contextual-targeting>>.

⁶¹⁹ See section 1.3.2.5 for an overview of the types of measurement data.

without an identifier, there is no way for an advertiser to connect a user's view or click on an ad with their purchase of a product. As the technology stands, the measure of engagement with an ad available to advertisers is clicks. Without the use of identifiers, advertisers and agencies are not able to measure reach, engagement and attribution in real time and would need to rely on alternative methods for measurement.

Three advertisers interviewed in the context of this study expressed concerns about not being able to measure reach, conversions or attribution when using contextual advertising⁶²⁰. As one of these advertisers mentioned, that means that it is difficult to "connect cause and effect" when using contextual advertising⁶²¹. Another one of these advertisers concurred that "no one can solve this basic question of reach for me [when using contextual advertising]. I haven't heard anyone. Just tell me how many browsers I reached"⁶²². A third advertiser highlighted how the lack of persistent identifiers limits attribution measurement: "when you use non-consented traffic, you don't know how you reached this person and how they came to your website. Did you reach them [with an ad] before they reached your website? You don't know that"⁶²³.

This may make it difficult for publishers to demonstrate the effectiveness of advertising on their sites and apps, which could in turn reduce advertiser demand. As one advertiser interviewed for this study mentioned, lack of access to measurement and attribution data could "make it more difficult for publishers to monetise their audiences in a granular fashion"⁶²⁴. As one publisher interviewed as part of this study said, "contextual [advertising] may not be sufficient; without some form of targeting, publishers will lose revenue"⁶²⁵. In particular, publishers could struggle to compete with large platforms that can generate measurement by tracking users in logged-in environments. As one publisher mentioned, if the current model of digital advertising were to end, "advertisers would flock to Google and [Meta]"⁶²⁶.

Contextual advertising's limitations when it comes to measurement data can partially be explained by the lack of investment in alternative ways of measuring the performance of advertising. According to Kobler's CEO Erik Bugge, "the industry could have started finding other ways of measuring the impact of ads without having all this personal data flowing around [when the GDPR was

⁶²⁰ Advertisers 1, 2 and 4.

⁶²¹ Advertiser 2.

⁶²² Advertiser 4.

⁶²³ Advertiser 1.

⁶²⁴ Advertiser 5.

⁶²⁵ Publisher 1.

⁶²⁶ Publisher 2.

adopted], but they chose not to. They are only now starting to come up with alternatives". The potential to measure engagement and conversions without third-party data sharing is being explored in the context of local profiling models⁶²⁷. It is therefore possible that further investment could result in more innovation in methods of measurement that rely less on tracking and profiling.

Conversely, as one advertiser interviewed for this study pointed out, the large revenues derived from the current digital advertising model means that its largest providers can spend a lot on research to help increase confidence in their tools, including to demonstrate effectiveness: "The platforms are really big, they've got tons of salespeople, they've got loads of money to throw around whether it's on publicists or on research"⁶²⁸.

The Digital Markets Act (DMA) introduces provisions designed to "further enhance fairness, transparency and contestability of online advertising services"⁶²⁹ by requiring gatekeepers to provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, with "access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data"⁶³⁰. These measures could go some way to improving the availability of data for advertisers and publishers to make evidence-based decisions, but some industry experts interviewed for this study have pointed to possible limitations of these provisions that would need to be addressed in order to meaningfully improve transparency in the digital advertising ecosystem. This is discussed in more detail in section 8.

5.1.3.5 Benefit of preventing ads appearing alongside disinformation and harmful content

Whereas the current digital advertising model involves the delivery of ads to specific users, contextual advertising can target specific contexts, which can contribute to advertisers having greater control over the content next to which their ads are placed (see section 2.2.1.2). For example, an ad for hiking shoes

⁶²⁷ See section 5.2.2.5.

⁶²⁸ Advertiser 2.

⁶²⁹ Recital 58 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁶³⁰ Article 6.8 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

delivered to a user interested in hiking under the current digital advertising model has the chance of reaching that user when they are visiting a website hosting harmful content, particularly when appropriate brand safety controls are not in place. Should the same ad be contextually targeted to a user when they visit a hiking website, the chances of the ad being displayed next to harmful content falls dramatically. Contextual advertising therefore acts similarly to technologies that are common in brand safety controls which advertisers already deploy to prevent or ensure that their ads do not appear next to certain content⁶³¹. Several brand safety vendors are even diversifying to provide contextual targeting as well. According to ad tech intermediary Rev·Amp, "since ads are only shown on relevant content, advertisers can trust that their ads won't be placed next to, before, or after content that will negatively impact their brand reputation"⁶³².

Using contextual information as the basis for brand safety efforts does have its drawbacks. For example, studies have shown that keyword-based exclusion lists can often be used in too crude a fashion, resulting in publishers and content that are not harmful losing ad revenue. For example, a 2019 study found that advertisers were using contextual keyword blocking to prevent ads from appearing in content that included or was related to the words "gay", "lesbian" and "bisexual" due to concerns around brand safety⁶³³. Additionally, keyword blocking has led to losses in revenues for publishers hosting content about the war in Ukraine⁶³⁴ and the COVID-19 pandemic⁶³⁵. Indeed, a Digiday survey found that 43% of media buyers (advertisers and their agencies) avoid advertising next to news content because of brand safety concerns⁶³⁶. According to contextual provider Seedtag, the use of NLP can enable "deep sentiment and tone analysis, going way beyond just placing keyword blocks on articles" and can at least partially remedy this issue⁶³⁷.

⁶³¹ See: 'Understanding Brand Safety & Brand Suitability in a Contemporary Media Landscape' (IAB, December 2020), p. 12 <<https://www.iab.com/wp-content/uploads/2020/12/IAB-Brand-Safety-and-Suitability-Guide-2020-12.pdf>>.

⁶³² Hemsworth F, 'Contextual Advertising For Publishers: Skyrocket Your Revenue' (RevAmp, 3 March 2022) <<https://revamp.softonic.com/blog/contextual-advertising-for-publishers-skyrocket-your-revenue/>>.

⁶³³ Baumatz U, 'How Keyword Blacklists Are Killing Reach and Monetization - A Study by CHEQ's Department of Data Science' (CHEQ, 2019) <<https://info.cheq.ai/hubfs/Research/Brand-Safety-Blocklist-Report.pdf>>.

⁶³⁴ McCarthy J, 'Media agencies struggling to keep brands advertising around bleak Ukraine news cycle' (The Drum, 1 March 2022) <<https://www.thedrum.com/news/2022/03/01/media-agencies-struggling-keep-brands-advertising-around-bleak-ukraine-news-cycle>>.

⁶³⁵ Sweney M, 'Newspapers to lose £50m in online ads as firms use coronavirus "blacklist"' (The Guardian, 1 April 2020) <<https://www.theguardian.com/media/2020/apr/01/newspapers-to-lose-50m-in-online-ads-as-firms-use-coronavirus-blacklist>>.

⁶³⁶ Weiss M, 'Digiday Research: 43 percent of media buyers say they avoid news content' (Digiday, 3 December 2018) <<https://digiday.com/marketing/digiday-research-43-percent-media-buyers-say-avoid-news-content/>>.

⁶³⁷ Gill D, 'How to achieve brand safety through contextual advertising' (The Drum, 26 April 2022) <<https://www.thedrum.com/profile/seedtag/news/achieving-brand-safety-through-contextual>>.

5.1.3.6 Limited availability of evidence on the impact on publisher revenues

Just as the evidence of contextual advertising's performance is limited (see section 5.1.3.2), so too is the evidence relating to its impact on publisher revenues, which primarily consists of case studies and surveys. The literature currently does not include any independent research on the impact of contextual advertising on publishers. Indeed, several publishers interviewed for this study indicated their concern around contextual advertising's ability to generate revenues⁶³⁸, with one noting that "if you take [ads based on profiling] completely away, the market will just decrease, and this money would be gone because advertisers wouldn't spend it anymore, because [contextual advertising] is not efficient for them"⁶³⁹. The fact that contextual advertising generates less measurement data is a key issue in this regard, as discussed in more detail in section 5.1.3.4 above. Additionally, the value that publishers are able to derive from their content as context can vary depending on the type of content produced, with news-related content potentially generating less revenue per impression.

One of the most commonly cited case studies is Dutch publisher NPO's experience with contextual advertising⁶⁴⁰. After switching to contextual advertising, NPO continued to see revenues grow between 9-27% each month, despite the shock of the COVID-19 pandemic. NPO saw impressions sold across its inventory grow by at least 83%. However, more case studies on a larger scale across different countries would be needed to conclude that these results could be replicated for all advertisers and publishers using contextual advertising. Discussing this case study specifically, one publisher interviewed for this study expressed scepticism regarding whether it was representative of the overall market saying, "It's one company out of a massive market, but which is very successful in this niche"⁶⁴¹.

Another case study shows that the New York Times generated as much revenue through contextual advertising in the first half of 2020 as it did during the whole of 2019 under the current digital advertising model⁶⁴². However, its contextual

⁶³⁸ Publishers 1 and 6.

⁶³⁹ Publisher 1.

⁶⁴⁰ Ryan J, 'Update (Six Months of Data): lessons for growing publisher revenue by removing 3rd party tracking' (*Brave Insights*, 24 July 2020) <<https://brave.com/publisher-3rd-party-tracking/>>.

⁶⁴¹ Publisher 1.

⁶⁴² Southern L, "'Supercharging contextual': Publishers eye potential for contextual ad revenue growth' (*Digiday*, 3 September 2020) <<https://digiday.com/media/supercharging-contextual-publishers-eye-potential-for-contextual-ad-revenue-growth/>>.

offering is “enriched” with first-party data collected from its users⁶⁴³, so it is not clear the extent to which the revenues involved can be attributed purely to contextual targeting alone.

Similar results have been reported based on surveys carried out by contextual advertising vendors. For example, Seedtag noted that publishers switching to contextual models can experience high incremental revenue growth⁶⁴⁴. A Rev·Amp survey reported that 59% of publishers say that advertisers are willing to pay more when they offer contextual advertising⁶⁴⁵. Here again, it is not clear whether this indicates contextual advertising free from or combined with targeting based on profiling. A survey by Connatix and Digiday found that 77% of publishers were able to offer contextual video advertising at prices on par with (38%) or higher than (39%) targeting based on profiling⁶⁴⁶. According to data shared by Kobler with the Greens-European Free Alliance (EFA) group in the European Parliament, “advertisers have consistently over a three-year period paid three times the average price for ad impressions through the Kobler platform across the +110 publisher sites in Norway and Sweden”⁶⁴⁷.

5.1.3.7 Fewer intermediaries than targeting based on profiling

Contextual advertising is often delivered programmatically, which means that it would not do away with some of the complexity associated with the current digital advertising model. That said, because contextual advertising does not rely on the use of identifiers, the number of intermediaries involved is typically smaller. For example, while multiple intermediaries can be involved in building profiles for targeting under the current model, few intermediaries are required to leverage a publisher’s context. For example, Kobler’s Erik Bugge noted that it is possible to “integrate [Kobler’s solutions] directly through header bidding, without intermediaries, or integrate through their supply-side platform (SSP). If you compare with other types of programmatic buying, it is clean”. This suggests that, for publishers, contextual advertising may require fewer intermediaries than targeting based on profiling.

⁶⁴³ Prabhat P, ‘To Serve Better Ads, We Built Our Own Data Program’ (*New York Times*, 17 December 2020) <<https://open.nytimes.com/to-serve-better-ads-we-built-our-own-data-program-c5e039bf247b>>.

⁶⁴⁴ Capdevila J, ‘The publishers’ guide to driving revenue-focused traffic’ (*Seedtag*, September 2021) <<https://www.seedtag.com/publishers-guide-contextual-advertising/>>.

⁶⁴⁵ Hemsworth F, ‘Contextual Advertising For Publishers: Skyrocket Your Revenue’ (*RevAmp*, 3 March 2022) <<https://revamp.softonic.com/blog/contextual-advertising-for-publishers-skyrocket-your-revenue/>>.

⁶⁴⁶ ‘The State of Contextual Targeting: Tactics, Technology and Revenue in 2021’ (*Connatix and Digiday*, August 2021) <<https://go.connatix.com/rs/733-VZA-777/images/resource-report-connatix-the-state-of-contextual-targeting.pdf>>.

⁶⁴⁷ McCann D, Stronge W and Jones P, ‘The Future of Online Advertising’ (*The Greens/EFA*, October 2021), p. 39 <<https://www.greens-efa.eu/files/assets/docs/surveillance-based-advertising-web.pdf>>.

Part of the difficulty in implementing contextual and URL embedding solutions can stem from difficulties with integrating into existing ad distribution and delivery systems. SVP of Strategy and Partnerships at Dstillery, Evan Hills, indicated that their solution was currently more difficult for advertisers to implement than digital advertising based on profiling. He noted that this is because platforms and intermediaries' advertiser user interfaces do not have integrated URL embeddings as options for advertisers to use, meaning that integration must be done "on the back end". Similarly, another alternative model provider interviewed for this study indicated that they had been unable to integrate within Google's Display & Video 360 (DV360), which is one of the most commonly-used demand-side platforms (DSPs) (see section 1.2.2.4.1). They noted that although Google was willing to integrate them into DV360, the process had so far lasted over two years: "the technical resources required on Google's side are significant, so they prioritise larger players: those that they are sure will drive enough revenue and clients for them to justify dedicating resources, like a product manager, to ensure it all goes smoothly". They suggested that this was a challenge likely faced by many smaller, newer players in the market. "If you're not connected to major platforms, then how can you attract new clients?"

5.1.3.8 Limited evidence of impact on pricing

As discussed in the previous section, the fact that contextual advertising can involve fewer intermediaries suggests it could be less costly for advertisers to use. That said, the evidence to support this point is limited. A study of four contextual advertising solutions by advertising agency GumGum found that for advertisers, the cost-per-click (CPC) and cost-per-mille (CPM) of using contextual targeting were lower than ads based on profiling (48% and 41% respectively)⁶⁴⁸. Nonetheless, there does not appear to be independent research to confirm GumGum's findings.

Pricing is necessarily a reflection of the different options available in the market. As outlined above, if there is a perception that contextual is somehow limited compared to the current digital advertising model (for example, because it offers less granular targeting) then it is logical that the price of contextual advertising is currently lower than other types. However, in a hypothetical market where more granular targeting options were not available, the relative pricing would likely shift, especially if demand levels were to change as well.

⁶⁴⁸ 'Contextual Targeting More Cost Efficient than Behavioral; GumGum Most Accurate Contextual Vendor' (*GumGum*, 6 September 2020) <<https://www.gumgum.com/press-releases/study-contextual-targeting-more-cost-efficient-than-behavioral-gumgum-most-accurate-contextual-vendor>>.

5.1.4 Popularity of contextual advertising

There is limited data available on the adoption of contextual advertising. The data that is available often does not distinguish between whether the solutions in question do or do not use contextual in combination with targeting based on profiling⁶⁴⁹.

Nonetheless, contextual advertising appears to be gaining in popularity. A survey by Connatix and Digiday suggests that 65% of advertisers are planning to increase their contextual-based budgets, that 44% of publishers “are already using context-based video ad tools themselves” or are “working with a third-party partner on contextual video solutions”, and that 15% of publishers are planning to explore roles for artificial intelligence in matching ads and content to audiences⁶⁵⁰.

The contextual advertising providers interviewed as part of this study suggested that the uptake of the model in the EU is currently low. When interviewed in April-May 2022, Kobler worked with 110 publishers in Norway and Sweden, Qwarry worked with 150 advertisers, and Opt Out Advertising worked with 20 publishers in the Netherlands. Eurostat data suggests that these are relatively small numbers, given that as many as 32% of advertisers in the EU use targeting based on profiling⁶⁵¹.

As URL embeddings are a more recent innovation, their adoption is significantly less widespread. When interviewed in May 2022, Dstillery, one of the main providers, offered URL embeddings to just 100 advertisers, and did not offer URL embeddings to any EU-based advertisers. It is not clear if Jellyfish, another key provider of URL embeddings, provides its model to any advertisers in the EU.

⁶⁴⁹ See for example: ‘Internet advertising of businesses - statistics on usage of ads’ (*Eurostat*, December 2018) <[https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet advertising of businesses - statistics on usage of ads](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads)> and ‘Contextual Advertising World Market Report’ (*StrategyR*, February 2022) <<https://www.strategyr.com/market-report-contextual-advertising-forecasts-global-industry-analysts-inc.asp>>.

⁶⁵⁰ ‘The State of Contextual Targeting: Tactics, Technology and Revenue in 2021’ (*Connatix* and *Digiday*, August 2021) <<https://go.connatix.com/rs/733-VZA-777/images/resource-report-connatix-the-state-of-contextual-targeting.pdf>>.

⁶⁵¹ ‘Internet advertising of businesses - statistics on usage of ads’ (*Eurostat*, December 2018) <[https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet advertising of businesses - statistics on usage of ads](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads)>.

5.2 Local profiling models

Local profiling models can reduce the privacy impact of digital advertising by reducing the amount of personal data that is shared with third parties, but they don't necessarily lead to less monitoring and profiling of individuals. These models can also involve the collection of sensitive data. Concerns have been raised that local profiling models could reduce transparency and competition in digital advertising.

Local profiling models store personal data about browsing behaviour on the individual's browser⁶⁵². This means that ads can be matched to users without personal data being shared with third parties.

The most widely used local profiling model currently available is Brave Ads, launched in 2019⁶⁵³. Additionally, Google's Privacy Sandbox is a collection of proposals which revolve around a local profiling model. The nature of these proposals is described in more detail below. Finally, a number of theoretical local profiling models have been also conceptualised by academics, including Adnostic⁶⁵⁴, Privad⁶⁵⁵ and more recently AdVeil⁶⁵⁶.

5.2.1 Google Privacy Sandbox

As discussed in section 1.3.1.2.2, Privacy Sandbox is an initiative launched by Google which aims to "develop a set of open standards to fundamentally enhance privacy on the web"⁶⁵⁷. As part of Privacy Sandbox, Google plans to "phase out" third-party cookies in Chrome in 2024⁶⁵⁸. Google has also indicated that Privacy Sandbox will be extended to its mobile operating system, Android⁶⁵⁹.

⁶⁵² It is possible that local profiling could be undertaken on a user's device (e.g. desktop or mobile), rather than their browser, but models available on the market currently operate on a browser-level.

⁶⁵³ 'An Introduction to Brave's In-Browser Ads' (*Brave*, 3 September 2020) <<https://brave.com/intro-to-brave-ads/>>.

⁶⁵⁴ Toubiana V and others, 'Adnostic: Privacy Preserving Targeted Advertising' (December 2010) <<https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf>>.

⁶⁵⁵ Guha S, Cheng B and Francis P, 'Privad: Practical Privacy in Online Advertising' (*Proceedings of 8th Symposium on Networked Systems Design and Implementation*, March 2011) <<https://people.mpi-sws.org/~francis/privad-nsdi11.pdf>>.

⁶⁵⁶ Servan-Schreiber S, Hogan K and Devadas S, 'AdVeil: A Private Targeted Advertising Ecosystem' (*Cryptology*, 2021) <<https://eprint.iacr.org/2021/1032.pdf>>.

⁶⁵⁷ Schuh J, 'Building a More Private Web' (*Google Blog*, 22 August 2019) <<https://www.blog.google/products/chrome/building-a-more-private-web/>> accessed 30 May 2022.

⁶⁵⁸ Goel V, 'An updated timeline for Privacy Sandbox milestones' (*Google Blog*, 24 June 2021) <<https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/>>; 'Expanding testing for the Privacy Sandbox for the Web' (*Google Blog*) <<https://blog.google/products/chrome/update-testing-privacy-sandbox-web/>>.

⁶⁵⁹ Chavez A, 'Introducing the Privacy Sandbox on Android' (*Google Blog*, 16 February 2022) <<https://blog.google/products/android/introducing-privacy-sandbox-android/>> accessed 30 May 2022.

Privacy Sandbox's collection of proposals and initiatives fall into three categories:

- **Ending third-party data sharing:** the overarching aim of Privacy Sandbox is to introduce prohibitions on third-party data sharing on Chrome and Android.
- **Targeting:** Privacy Sandbox includes proposals for targeting based on profiling that do not rely on sharing personal data with third parties.
- **Measurement:** Privacy Sandbox includes proposals for measuring the effectiveness of digital advertising campaigns that do not involve sharing personal data with third parties. This is the purpose of proposals such as the Attribution Reporting API.

This section will review the Privacy Sandbox proposals as a group, with reference to individual proposals where relevant. These proposals are primarily spearheaded by Google but discussed by a wide variety of stakeholders in the context of the World Wide Web Consortium (W3C), an international web standards organisation⁶⁶⁰. These stakeholders, which include primarily digital advertising intermediaries and ad tech experts, as well as a minority of publishers and advertisers, can review Google's proposals and propose changes. The W3C is also considering proposals that are not led by Google (see section 5.3). This process is evolving constantly, and it is possible that some proposals will be dismissed and new proposals added. As a result, the purpose of this review is not to provide an exhaustive analysis of the current status of each proposal. Rather, the objective is to identify any potential alternative models that are emerging as part of the process that could meet the criteria of (a) not relying on the monitoring and profiling of users, (b) not relying on the use of special category data (as set out in Article 9 GDPR) (c) not involving the sharing of data with multiple third parties.

5.2.2 Evaluation

5.2.2.1 Use of personal data

Brave Ads operates a local profiling model that does not rely on any third-party data sharing. That said, data collected by third parties could feasibly be used to enrich locally created profiles. For example, the AdVeil⁶⁶¹ local profiling model was

⁶⁶⁰ More specifically, Google's proposals are considered in the Improving Web Advertising Business Group (IWA-BG), the Privacy Community Group (PCG) or the Web Incubator Community Group (WICG). See Kihn M, 'What's Really Going On In the Privacy Sandbox?' (*AdExchanger*, 15 February 2022) <<https://www.adexchanger.com/data-driven-thinking/whats-really-going-on-in-the-privacy-sandbox/>>

⁶⁶¹ Servan-Schreiber S, Hogan K and Devadas S, 'AdVeil: A Private Targeted Advertising Ecosystem' (*Cryptology*, 2021) <<https://eprint.iacr.org/2021/1032.pdf>>.

designed to work with any browser, including ones that enrich locally created profiles with additional personal data.

Similarly to Brave Ads, all of the Privacy Sandbox proposals currently under discussion would prevent third-party data sharing. However, monitoring and profiling users would remain a key part of these models, including the use of sensitive data, albeit by one first party (in this case, Google) rather than a plethora of third parties.

The following evaluation of the use of personal data by local profiling models therefore assumes they are used without recourse to personal data collected by third parties.

5.2.2.1.1 Monitoring and profiling

Local profiling models rely on the profiling and monitoring of users as the basis for targeting, mostly through observing browsing behaviour data (e.g. websites visited, search queries). However, the scale of data collection is limited compared to the current digital advertising model because multiple third parties are usually not involved.

The current state of Privacy Sandbox proposals suggests that Google will continue to profile and monitor users for digital advertising purposes, but that third parties will no longer be able to. Topics API⁶⁶² and FLEDGE⁶⁶³, which together comprise Privacy Sandbox's primary targeting proposal, will see Chrome build profiles of users' interests based on their browsing behaviour. These profiles will become the basis of the "topics" on which users will be targeted (see section 5.2.2.3 for more detail).

Civil society and industry experts have raised concerns regarding the scale of the monitoring and profiling that Google would continue to carry out under proposals such as Topics API, FLEDGE and their shelved precursor, Federated Learning of Cohorts (FLoC)⁶⁶⁴. To address some of these concerns relating to Topics API's profiling and monitoring, Google has proposed the following steps:

⁶⁶² Goel V, 'Get to know the new Topics API for Privacy Sandbox' (*Google Blog*, 25 January 2022) <<https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>>.

⁶⁶³ Dutton S, 'FLEDGE API' (*Chrome Developers*, 27 January 2022) <<https://developer.chrome.com/docs/privacy-sandbox/fledge/>>.

⁶⁶⁴ See for instance 'Google's FLoC Is a Terrible Idea' (*Electronic Frontier Foundation*, 10 March 2021) <<https://edri.org/our-work/google-floc-is-a-terrible-idea/>>; Ryan J, '4 Big Questions about Google's new privacy position' (*Irish Council for Civil Liberties*) <<https://www.iccl.ie/digital-data/4-big-questions-about-googles-new-privacy-position/>>; von Tetzchner J, 'Heads up: Google's going off Topics again' (*Vivaldi*, 27 January 2022) <<https://vivaldi.com/blog/technology/heads-up-googles-going-off-topics-again/>>; 'Google's Topics API: Rebranding FLoC Without Addressing Key Privacy Issues' (*Brave*, 26

- **Time-limits:** only browsing data from the previous three weeks is used to determine interest topics.
- **K-anonymity:** when assigning topics to users, Google plans to introduce a 5% probability that a random topic is assigned. The aim is to hinder the identification of specific users⁶⁶⁵.

Additionally, Google has made several binding commitments to the UK Competition and Markets Authority (CMA) regarding its use of data after the phasing out of third-party cookies on Chrome. The company has pledged not to use personal data from a user's Chrome browsing history or Google Analytics account in its ad systems for the purposes of tracking that user "for the targeting or measurement of digital advertising on either Google owned and operated ad inventory or ad inventory on websites not owned and operated by Google"⁶⁶⁶. In developing Privacy Sandbox as a whole, these commitments also bind Google to design and implement features with consideration to the "impact on privacy outcomes and compliance with data protection principles as set out in the Applicable Data Protection Legislation"⁶⁶⁷.

5.2.2.1.2 Sensitive data

Because local profiling models rely on monitoring and profiling to target ads to users, it is possible that special category data could be collected in the process.

As part of Topics API and FLEDGE, it is possible that Google would be able to collect users' sensitive data in the course of monitoring them and creating profiles of their interests. One measure proposed by Google to avoid processing special category data is that the taxonomy of topics used for targeting should exclude "sensitive" topics. According to Google, "The Topics taxonomy will be public and human-curated to avoid sensitive categories"⁶⁶⁸.

January 2022) <<https://brave.com/web-standards-at-brave/7-googles-topics-api/>> and Claburn T, 'Google's FLoC flopped, boffins claim, because it failed to provide promised privacy' (*The Register*, 5 May 2022) <https://www.theregister.com/2022/05/05/googles_floc_flopped_boffins_claim/>.

⁶⁶⁵ See also section 5.3.1.1.

⁶⁶⁶ 'Competition and Markets Authority Case 50972 - Privacy Sandbox Google Commitments Offer' (4 February 2022)

<https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf>.

⁶⁶⁷ The "applicable legislation" refers to the UK GDPR, Data Protection Act 2018, and Privacy and Electronic Communications (EC Directive) Regulations 2003.

⁶⁶⁸ Dutton S, 'The Topics API' (*Chrome Developers*, 25 January 2022

<<https://developer.chrome.com/docs/privacy-sandbox/topics/#sensitive-topics>>.

However, these proposed safeguards have received criticism. In particular, issue has been taken with Google setting itself as the arbiter of what information is considered “sensitive”. Importantly, context largely dictates whether information is sensitive to a particular user. As a reference point for which topics it will ultimately use, Topics API developers have turned to the IAB Tech Lab Audience Taxonomy⁶⁶⁹. Peter Snyder, Senior Director of Privacy at Brave, has pointed out that certain categories which appear innocuous at face value might carry underlying sensitivities. For example, categories such as “alcoholic beverages” might be sensitive in certain religious communities and “job market” could be sensitive to someone who is already employed⁶⁷⁰. “There is no such thing as categorically non-sensitive data” he noted⁶⁷¹.

Article 26 DSA introduces a prohibition on providers of online platforms to present on their interfaces advertising “based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679”⁶⁷². Google already claims to restrict the use of “sensitive interest categories” in “personalised ads”⁶⁷³. Many of Google’s restrictions align broadly with the GDPR’s definition of special category data, although it is not clear to what extent this includes categories that could be used to infer sensitive characteristics indirectly. Similarly, some civil society stakeholders consulted for this study expressed concern that the wording of Article 26.3 DSA is not sufficiently precise to prohibit non-special category data from being combined and inferred to create new targeting options which could be considered sensitive, for example targeting individuals based on an interest in certain topics known to be linked – albeit not explicitly – to areas such as sexual orientation, religion or health.

5.2.2.1.3 Third-party data sharing

The personal data underlying local profiling is collected and processed locally. In theory, it is not shared with third parties, nor enriched with third-party data.

⁶⁶⁹ ‘The Topics API’ (*GitHub*) <<https://github.com/patcg-individual-drafts/topics>>.

⁶⁷⁰ ‘Google shouldn’t decide what you consider sensitive’ (*Brave*, 26 January 2022) <<https://brave.com/web-standards-at-brave/7-googles-topics-api/#google-shouldnt-decide-what-you-consider-sensitive>>.

⁶⁷¹ ‘Google shouldn’t decide what you consider sensitive’ (*Brave*, 26 January 2022) <<https://brave.com/web-standards-at-brave/7-googles-topics-api/-google-shouldnt-decide-what-you-consider-sensitive>>.

⁶⁷² Article 26.3 of the Digital Services Act. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁶⁷³ ‘Personalized Advertising’ (*Advertising Policies Help*) <<https://support.google.com/adspolicy/answer/143465?hl=en>> accessed 9 September 2022.

Indeed, as discussed above, the overarching aim of Privacy Sandbox is to “phase out support for third-party cookies”⁶⁷⁴. In theory, this means that no third-party data sharing should occur when users are served ads through Google Chrome and Android, as is currently the case for Brave users.

As well as blocking third-party cookies and mobile identifiers, another proposal by Google called Privacy Budget⁶⁷⁵ would place limits on the ability of intermediaries and publishers to track users through fingerprinting⁶⁷⁶. This proposal has nonetheless received criticism, including on the definition of the budget scope (i.e. how much personal data could be collected in practice) and vulnerability to exploitation⁶⁷⁷.

Additionally, some of Google’s proposals in this area have been criticised for placing limits on users’ ability to block tracking through browser extensions. Brave⁶⁷⁸ and the Electronic Frontier Foundation (EFF)⁶⁷⁹ have pointed out that Google’s Manifest V3 proposal would weaken the ability of browser extensions to block trackers, including the ones set by Google.

Finally, several Privacy Sandbox proposals such as FLEDGE rely on “trusted servers” for some of their data processing, which Googles notes are “defined by compliance with certain principles and policies”⁶⁸⁰. As explained by Johnny Ryan, Senior Fellow at the Irish Council for Civil Liberties, Google has not properly defined the nature and governance of trusted servers, nor how they will ensure that personal data is not shared with third parties⁶⁸¹.

Potentially as a result of these concerns, certain advertisers and publishers interviewed as part of this study questioned whether Privacy Sandbox would lead

⁶⁷⁴ Goel V, ‘An updated timeline for Privacy Sandbox milestones’ (*Google Blog*, 24 June 2021) <<https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/>>.

⁶⁷⁵ Privacy Budget would estimate users’ “fingerprinting surfaces” (i.e. points where information is revealed about a user or device, for example screen resolution) and introduce a “maximum tolerance” which would limit the amount of data that is exposed when a user visits a site. A site would be allowed to collect up to a certain amount of data, as defined by Google, called the “budget”. Any attempt to collect data beyond this allocation would fail. See Rescorla E, ‘Analysis of Google’s Privacy Budget Proposal’ (*Mozilla*, 1 October 2021) <<https://blog.mozilla.org/en/mozilla/google-privacy-budget-analysis/>>.

⁶⁷⁶ See section 1.3.1.1.3.

⁶⁷⁷ ‘Brave, Fingerprinting, and Privacy Budgets’ (*Brave*, 6 November 2019) <<https://brave.com/web-standards-at-brave/2-privacy-budgets/>>.

⁶⁷⁸ ‘Privacy And Competition Concerns with Google’s Privacy Sandbox’ (*Brave*, 26 January 2022) <<https://brave.com/web-standards-at-brave/6-privacy-sandbox-concerns/>>.

⁶⁷⁹ Barnett D, ‘Chrome Users Beware: Manifest V3 is Deceitful and Threatening’ (*Electronic Frontier Foundation*, 9 December 2021) <<https://www.eff.org/deeplinks/2021/12/chrome-users-beware-manifest-v3-deceitful-and-threatening>>.

⁶⁸⁰ Bindra C, ‘Building a privacy-first future for web advertising’ (*Google Blog*, 25 January 2021) <<https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/>>.

⁶⁸¹ Ryan J, ‘4 Big Questions about Google’s new privacy position’ (*Irish Council for Civil Liberties*) <<https://www.iccl.ie/digital-data/4-big-questions-about-googles-new-privacy-position/>>.

to real improvements on privacy. One advertiser suggested that advertisers' expectations regarding how privacy-friendly Topics API would be have "decreased over time"⁶⁸². Similarly, a publisher mentioned that they were "not interested" in technologies that just replicate the "current data-driven model", as they expected these to be "banned as well"⁶⁸³.

It is worth noting that the local profiling model, insofar as it prevents the sharing of data with third parties, could be considered to apply Article 10 of the European Commission's Proposal for an ePrivacy Regulation by default⁶⁸⁴. Indeed, both Brave and the Privacy Sandbox "prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment". When using both of these browsers, users would therefore not have the option of allowing this form of third-party data sharing.

5.2.2.2 Limited independent evidence to assess the effectiveness of local profiling models

According to Brave, at 8%, the average click-through rate (CTR) for Brave Ads campaigns is significantly higher than the market average^{685, 686}. A Brave study of several campaigns found that brand recall was on average 49% higher compared with ads on "traditional online advertising platforms"⁶⁸⁷. Brave has also documented various other campaign objective successes within its case studies⁶⁸⁸. However, there is a lack of independent data to verify the effectiveness of local profiling models in general.

As Privacy Sandbox's projects are still in the form of proposals, it is currently not possible to assess their performance in comparison with the current digital advertising model. Although tests for proposals such as Topics API, FLEDGE and

⁶⁸² Advertiser 5.

⁶⁸³ Publisher 2.

⁶⁸⁴ Article 10 ePrivacy Regulation proposes requiring that "software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment". Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD), <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>>.

⁶⁸⁵ 'Brave Passes 50 Million Monthly Active Users, Growing 2x for the Fifth Year in a Row' (*Brave*, 25 January 2022) <<https://brave.com/2021-recap/>>.

⁶⁸⁶ 'Nexo Case Study' (*Brave*) <<https://brave.com/brave-ads/casestudies/nexo/>>

⁶⁸⁷ 'Engaging with New "Ad-Choosers"' (*Brave* and *dentsu international*, March 2021) <<https://brave.com/static-assets/files/Engaging-With-Ad-Choosers.pdf>>.

⁶⁸⁸ 'New Brave Ads Use Cases Show Up to 15.8% Click-Through Rate, Unmatched Engagement' (*Brave*, 14 September 2020) <<https://brave.com/brave-ads-use-cases/>>.

Attribution Reporting API began in April 2022⁶⁸⁹, the results had not been made publicly available at the time of writing.

5.2.2.3 Targeting

This section will begin with an overview of how targeting takes place under local profiling models, including under the Privacy Sandbox proposals. It will then assess concerns that have been raised by industry stakeholders regarding the effectiveness of this kind of targeting.

5.2.2.3.1 Targeting under the local profiling model

As noted above, local profiling models operate on the basis of profiles of users based on data collected locally by the browser.

Under Brave Ads, the Brave browser uses machine learning to process a user's browsing data (e.g. pages visited, search queries) in order to determine a user's areas of interest. Advertisers that work with Brave send their ads to Brave's ad server, where they are added to a catalogue. This catalogue is periodically downloaded to the user's device (rather than in real time per impression, as is the case in the current digital advertising model). These ads are then delivered to users based on the interest categories determined by the browser, but these interest categories are not sent to Brave's ad servers or to any third parties. AdVeil's proposal model works in a similar fashion to Brave's, although interest categories are shared anonymously with third parties.

With regards to Google's Privacy Sandbox, Topics API is the primary proposal related to targeting⁶⁹⁰. Topics API involves targeting users based on a profile of their interests⁶⁹¹. Like Brave's model, these profiles are built within the browser using personal data about users' browsing behaviour. Under the current Topics API proposal, Google will assign up to three high-level categories to websites based on the content they host (e.g. "news" to a news publisher, "fashion" to a fashion magazine). When users browse the web, their browser will keep a record of their interest categories and assign up to three categories to them for a maximum period of three weeks. When users are served an ad through Chrome,

⁶⁸⁹ 'What to Expect from Privacy Sandbox Testing' (*Chromium Blog*, 31 March 2022) <<https://blog.chromium.org/2022/03/what-to-expect-from-ps-testing.html>>.

⁶⁹⁰ Goel V, 'Get to know the new Topics API for Privacy Sandbox' (*Google*, 25 January 2022) <<https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>>.

⁶⁹¹ This framework was initially introduced by Google as part of the Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE) proposal. 'TURTLEDOVE' (*GitHub*) <<https://github.com/WICG/turtledove/blob/main/Original-TURTLEDOVE.md>>.

these three categories would serve as the basis for targeting. Google has also suggested that Topics API might also complement contextual targeting⁶⁹².

As a separate proposal from Topics API, FLEDGE would also allow interest-based targeting without the use of third-party data sharing. Its primary use-case is re-targeting: targeting users with ads based on their visits to specific advertiser websites. Under the FLEDGE proposal, advertisers' websites are able to request that the Chrome browser add a user to a relevant interest group held within the browser, following that user's visit to their website. This information, which is the basis for targeting, is collected and stored within centralised "trusted servers"⁶⁹³. When a user visits a publisher's website, FLEDGE would run an internal auction within the trusted server to select an ad based on the interest categories that the user has been added to.⁶⁹⁴ Ads are displayed within a "fenced frame"⁶⁹⁵ which theoretically prevents a webpage from learning about the contents of the ad, and consequently a user's interests⁶⁹⁶.

Google has also issued a proposal for the use of lookalike audiences (i.e. targeting ads to users that share similar characteristics as current customers) titled Similar Cohort Audiences Upholding Privacy (SCAUP)⁶⁹⁷. Under SCAUP, the browser uses browsing data to create profiles of users and encrypts these profiles using secure multi-party computing (MPC)⁶⁹⁸, which involves encryption through the use of two trusted servers. These servers use the data in question to train targeting models to predict whether a user should be part of a similar audience group. According to Google, "neither MPC server alone can decrypt the training or test data, they operate on top of the encrypted data only"⁶⁹⁹. Periodically, a user's browser would query the MPC servers to determine whether there are any similar-audience groups that the browser should join. The MPC servers then invite the browser to join the appropriate interest groups (i.e. the same interest groups as created under the Topics API framework).

Advertisers and regulators have raised concerns regarding how precisely advertisers will be able to target users when using Privacy Sandbox's targeting-

⁶⁹² Dutton S, 'The Topics API' (*Chrome Developers*, 25 January 2022) <<https://developer.chrome.com/docs/privacy-sandbox/topics/>>.

⁶⁹³ See section 5.2.2.1.3.

⁶⁹⁴ Schiff A, 'AdExplainer: Meet The FLEDGE API' (*AdExchanger*, 18 April 2022) <<https://www.adexchanger.com/adexplainer/adexplainer-meet-the-fledge-api/>>.

⁶⁹⁵ 'Fenced Frames' (*GitHub*) <<https://github.com/WICG/fenced-frame>>.

⁶⁹⁶ Jack J and others, 'Fenced Frames' (*Chrome Developers*, 7 March 2022) <<https://developer.chrome.com/docs/privacy-sandbox/fenced-frame/>>.

⁶⁹⁷ 'Similar Cohort Audiences Upholding Privacy' (*GitHub*) <<https://github.com/google/ads-privacy/tree/master/proposals/scaup>>.

⁶⁹⁸ See section 5.3.1.1.

⁶⁹⁹ 'Similar Cohort Audiences Upholding Privacy' (*GitHub*) <<https://github.com/google/ads-privacy/tree/master/proposals/scaup>>.

related proposals. For example, current documentation on Topics API⁷⁰⁰ suggests that there will be 350 initial topics – a relatively small number which could limit how precisely advertisers are able to target their products⁷⁰¹. Google has stated that the number of interest groups is intentionally small, to “reduce the chance that individuals could be identified based on their unique topics of interest”⁷⁰². David Dykes, Director of Media at advertising agency Baldwin&, noted that this would have little effect on larger brands engaging in more generic awareness-based campaigns, but could disadvantage smaller campaigns that might be more reliant on precision to advertise a niche product⁷⁰³. As the CMA points out in its investigation into Google’s Privacy Sandbox, “although the Privacy Sandbox Proposals would allow publishers to offer advertisers the ability to provide some degree of personalised advertising on their ad inventory, this will be less granular and less personalised”⁷⁰⁴.

Google has directly responded to the issue of imprecise targeting in its first quarterly update to Privacy Sandbox (mandated by the CMA commitments). Google states that the “usefulness of the API will be explored through testing” and that the taxonomy will “evolve based on testing results”⁷⁰⁵. Development of Privacy Sandbox remains an ongoing process and, with origin trials having only started recently, it remains too early to tell if the dialogue envisaged by the CMA will be an effective mechanism for protecting all stakeholder interests.

Whereas the current digital advertising model allows publishers and intermediaries to offer advertisers different targeting criteria, both Brave and Privacy Sandbox’s proposed local profiling models see targeting criteria defined by the browser. Industry figures such as Christer Ljones, Head of Data at Schibsted Marketing Services, have raised concerns about this, noting that “we can’t accept Google’s

⁷⁰⁰ Dutton S, ‘The Topics API’ (*Chrome Developers*, 25 January 2022)

<<https://developer.chrome.com/docs/privacy-sandbox/topics/>>.

⁷⁰¹ For instance, critics have pointed out that Topics might be unable to differentiate between a user with an interest in walking boots and one with an interest in football boots. See ‘Google unveils latest cookie replacement. Here’s what marketers are saying’ (*The Trade Desk*, 3 February 2022)

<<https://www.thetradedesk.com/us/news/google-unveils-latest-cookie-replacement-heres-what-marketers-are-saying>>.

⁷⁰² ‘Topics: The new Privacy Sandbox proposal for interest-based advertising’ (*Google Support*, 22 February 2022) <<https://support.google.com/google-ads/answer/11899856>>.

⁷⁰³ ‘Google unveils latest cookie replacement. Here’s what marketers are saying’ (*The Trade Desk*, 3 February 2022) <<https://www.thetradedesk.com/us/news/google-unveils-latest-cookie-replacement-heres-what-marketers-are-saying>>.

⁷⁰⁴ ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972’ (*CMA*, 11 February 2022), p. 37

<https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷⁰⁵ Merewood R, ‘Feedback Report - 2022 Q1’ (*Chrome Developers*, 17 May 2022)

<<https://developer.chrome.com/docs/privacy-sandbox/feedback/report-2022-q1/>> accessed 1 June 2022.

business interest dictating that segment list⁷⁰⁶. Furthermore, although Google has suggested that the taxonomy of Topics API could be open sourced or even maintained externally, the collection of browsing data necessary to assign interest categories to users will depend on Google. Companies that spoke to the CMA have suggested that “this is likely to lead to a homogenisation of ad inventory and ad tech services and would reduce the ability of rivals to provide a value proposition⁷⁰⁷”.

In its CMA commitments, Google agreed to publish a “dedicated microsite” with a “process for stakeholder engagement”. Stakeholder feedback is to be included and addressed in publicly available quarterly reports. In the first of these reports, Google acknowledged concerns about its role in determining the Topics API taxonomy, responding that “Chrome remains open to input on the taxonomy” and stating its interest in discussing how industry bodies “can play a more active role in developing and maintaining the taxonomy in the long term⁷⁰⁸”. It is unclear whether the broad nature of this commitment will satisfy industry stakeholders. As with many of its CMA commitments, the extent to which Google will allow advertisers and publishers to meaningfully impact the development of the Privacy Sandbox will become clearer only over time.

5.2.2.4 Reach

The reach of local profiling models is limited to the number of people that use the browser in question. For example, Brave had 50.2 million monthly active users in 2021⁷⁰⁹, while Google Chrome has 2.65 billion⁷¹⁰. This large difference is likely to be a significant factor for many advertisers, given the importance that they place on reach (see section 4.1.1).

From a publisher standpoint, the impact of local profiling models on the number of users that publishers can reach with ads depends on how they are implemented. Brave’s model essentially implies that only publishers that are part of Brave’s

⁷⁰⁶ Joseph S, ‘With Google’s latest Privacy Sandbox update, European publishers see silver lining’ (*Digiday*, 9 February 2022) <<https://digiday.com/media/with-googles-latest-privacy-sandbox-update-european-publishers-see-silver-lining/>>.

⁷⁰⁷ ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972’ (*CMA*, 11 February 2022), p. 38 <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷⁰⁸ Merewood R, ‘Feedback Report - 2022 Q1’ (*Chrome Developers*, 17 May 2022) <<https://developer.chrome.com/docs/privacy-sandbox/feedback/report-2022-q1/>> accessed 1 June 2022.

⁷⁰⁹ ‘Brave Passes 50 Million Monthly Active Users, Growing 2x for the Fifth Year in a Row’ (*Brave*, 5 January 2022) <<https://brave.com/2021-recap/>>.

⁷¹⁰ Dean B, ‘Google Chrome Statistics for 2022’ (*Backlinko*, 8 March 2021) <<https://backlinko.com/chrome-users>>.

Creators programme can generate revenues from the Brave users that visit their websites. This may change in the future, as Brave plans to introduce a publisher ads program, which would allow publishers that have joined the Creators to host ads directly on their interface. Conversely, as Privacy Sandbox proposals currently stand, publishers should (in theory) see no difference in the number of Chrome users that they can reach with their ads.

Current local profiling models such as Brave Ads involve counting impressions without the use of identifiers⁷¹¹. This means that although it is possible to count those impressions, it is not possible to measure how many individual users have seen a particular ad (“frequency”). This is also the case for the AdVeil model⁷¹². Conversely, Google has stated that measuring how many individual users have been reached in a campaign will remain possible under Privacy Sandbox proposals through the Attribution Reporting API⁷¹³.

5.2.2.5 Browser-defined methods of measuring the effectiveness of campaigns

When using local profiling models, the extent to which an advertiser can measure the effectiveness of campaigns depends on the browser’s capabilities. In all cases though, it appears that local profiling models allow the collection of less measurement data than the current digital advertising model. For example, Brave states that Brave Ads can measure clicks, impressions, conversions⁷¹⁴ and a range of “attention metrics” without using personal data⁷¹⁵. However, it is not possible to measure reach or frequency. Meanwhile, with Privacy Sandbox proposals as they currently stand, Google has said that advertisers would still be able to measure the effectiveness of their campaigns, as all relevant measurement data should remain available to them, albeit potentially on a more limited scale. The

⁷¹¹ ‘Security and privacy model for ad confirmations’ (*GitHub*) <<https://github.com/brave/brave-browser/wiki/Security-and-privacy-model-for-ad-confirmations>>.

⁷¹² Servan-Schreiber S, Hogan K and Devadas S, ‘AdVeil: A Private Targeted Advertising Ecosystem’ (*Cryptology*, 2021) <<https://eprint.iacr.org/2021/1032.pdf>>.

⁷¹³ See section 5.2.2.5.

⁷¹⁴ In Brave, conversions are measured strictly within the browser, with the help of a “conversion page” defined by the advertiser (e.g. a page thanking the user for a purchase). Attribution can be measured on a click-through or view-through basis, with the browser being able to associate a user’s view of an ad with their landing on the associated “conversion page”. Upon the delivery of an ad, “the browser begins a countdown specified in the attribution window, and if the browser sees that the user has visited the conversion page within that period of time, it counts the conversion one time for the user”. Brave safeguards user privacy in this context by reporting conversions to the Brave Ads server on an anonymous basis, without any identifier. See ‘Brave Conversion and Attribution Guide’ (*Brave*, 2020) <https://docs.google.com/document/d/15Wvzov1Jn8r9etL_EoAxM5k9tlczZMsjiCHhjACj-o8/edit>.

⁷¹⁵ ‘Brave Ads Media Kit’ (Brave) <https://brave.com/brave-ads/assets/Brave_Media_Kit.pdf>.

Attribution Reporting API⁷¹⁶ is Privacy Sandbox's primary measurement proposal. It enables advertisers to measure conversions⁷¹⁷, although Google has warned that it may be less granular than existing methods of measurement. Though beneficial from a privacy-perspective, this could see less granular conversion data for advertisers (Google has stated that the API will not support conversion-side data such as conversion price or conversion time)⁷¹⁸. A combination of techniques including differential privacy are also used to reduce the risk of re-identification^{719, 720}.

The CMA concurs that the Attribution Reporting API could see more limited measurement than under the current model, making it harder for advertisers to gauge the effectiveness of campaigns⁷²¹. The CMA concludes that this could hinder rival intermediaries' ability to demonstrate the effectiveness of their services and their ability to optimise campaigns in real time. In its first quarterly progress report to the CMA on the Privacy Sandbox, Google highlighted that the accuracy of measurement data was an important concern raised by industry stakeholders⁷²². Its response acknowledges that "noise based privacy protections have greater impact on smaller data slices" but suggests that small data samples (of one or two purchases) may lack utility to advertisers anyway, and that aggregating data over a longer period of time could remedy this issue.

Additionally, as the CMA points out, Google already has a conflict of interest in controlling the largest ad server and DSPs, with the company "marking its own homework" in measuring and reporting successful ad delivery⁷²³. The CMA notes that "while advertisers currently have the possibility to choose an independent advertiser ad server, they would have very limited influence over the web browser chosen by web users"⁷²⁴.

⁷¹⁶ Dutton S and Nalpas M, 'Attribution Reporting' (*Chrome Developers*, 27 May 2022) <<https://developer.chrome.com/docs/privacy-sandbox/attribution-reporting/>> accessed 31 May 2022.

⁷¹⁷ See section 1.3.2.5.6.

⁷¹⁸ Nalpas M and Dutton S, 'Attribution Reporting' (*Chrome Developers*, 18 May 2021)

<<https://developer.chrome.com/docs/privacy-sandbox/attribution-reporting/>>.

⁷¹⁹ See section 5.3.1.1.

⁷²⁰ Dutton S, 'Digging into the Privacy Sandbox' (*web.dev*, 25 January 2022) <<https://web.dev/digging-into-the-privacy-sandbox/>>.

⁷²¹ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022), p. 31-39

<https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷²² 'Privacy Sandbox Progress Report, prepared for the CMA' (*Google*, 16 May 2022)

<https://assets.publishing.service.gov.uk/media/62835bfee90e071f6af1457e/Privacy_Sandbox_Progress_Report_to_the_CMA_2022_Q1.pdf>.

⁷²³ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022), p. 47

<https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷²⁴ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022),

Article 6.8 DMA is designed to “further enhance fairness, transparency and contestability of online advertising services”⁷²⁵ by requiring gatekeepers to provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, with “access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data”⁷²⁶. These measures could go some way to improving the availability of data for advertisers and publishers to make evidence-based decisions, but some industry experts interviewed for this study have pointed to possible limitations of these provisions that would need to be addressed in order to meaningfully improve transparency in the digital advertising ecosystem. This is discussed in more detail in section 8.

5.2.2.5.1 Less data available for publishers to prove their value

Local profiling models largely fall short in addressing the concerns raised by publishers with regards to the data they feel they need to compete with large platforms for access to ad revenue (see section 4.4.1). Publishers are primarily concerned about the limits which Google plans to introduce on third-party data sharing, which they feel could limit their ability to monetise their audiences and prove the value of their services to advertisers.

Blocking third-party data sharing could increase the value of first-party data, as this may become the only kind of data that publishers are able to collect about their users. Indeed, most publisher respondents said that they had started work to increase their store of first-party data, such as by developing larger logged-in ecosystems and premium content that they can monetise through subscriptions. That said, publishers’ ability to compete with large platforms when it comes to reach is limited, as large platforms’ userbases are likely to remain larger given their already significant advantage in this area. Indeed, the CMA notes that without due scrutiny, Google could more effectively leverage first-party tracking than competitors, due in part to its “user facing services” and ability to connect data from logged in users. The CMA argues that this could harm the ability of

p.47 <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷²⁵ Recital 58 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁷²⁶ Article 6.8 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

“publishers to sell ad inventory to advertisers in competition with Google’s ad inventory”⁷²⁷. That also means that publishers’ concerns regarding their inability to compete with Google on a price-level would likely remain, and publishers’ limitations in relation to data and reach would continue to contribute to increases in their costs and therefore the price of advertising on their platforms (see section 4.4.3). However, it is important to note that gatekeepers would still be able to combine and/or cross-use data across services if the user has “been presented with the specific choice and has given consent”. Some stakeholders speculated that Google would likely retain an advantage under current Privacy Sandbox proposals if users provide consent in this way.

The DMA may partially address this by prohibiting companies designated as gatekeepers from combining and/or cross-using personal data across different services they provide: this is seen by some stakeholders as an effective way to restrict large platforms’ ability to gain a competitive advantage by leveraging the large amounts of data generated by individuals across the different services they provide. This, some stakeholders argue, would enable publishers that collect first-party data from their readers to compete more effectively with large platforms.

The Brave browser currently does not share any data with publishers on the performance of ads, since ads are not shown within the publishers’ interface. This may change when Brave begins allowing publishers to display ads within its interface. At this point, the levels of data available to publishers would be smaller than under the current digital advertising model because of the limits Brave places on third-party tracking.

5.2.2.6 Browser-dependent tools to prevent ads appearing alongside disinformation and harmful content

The extent to which local profiling models can deal with problems related to ads being placed next to harmful content or disinformation depends on the controls put in place by the browser. Because ad delivery happens within the browser, the extent to which third-party brand safety controls and verification intermediaries can be used is limited.

Remuneration of Brave Ads is currently not directly linked to publisher content. This is because Brave Ads are not displayed within publishers’ pages, but rather as push notifications within the browser or as “sponsored images” within new tabs opened by users. However, this does not necessarily prevent ad revenue from

⁷²⁷ ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972’ (*CMA*, 11 February 2022), p. 47
<https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

funding harmful content. Under the Brave model, Brave Rewards sees publishers automatically tipped by users when they collect Basic Attention Tokens (BATs) as a reward for paying attention to ads and clicking on them. It is not clear whether Brave puts any limits on which publishers can receive remuneration this way⁷²⁸, meaning that ad spend could still indirectly fund harmful content or misinformation through Brave, albeit on a more indirect basis.

The Privacy Sandbox proposals for brand safety controls illustrate the risks associated with placing limits on third-party brand safety controls. Companies who spoke to the CMA raised concerns that the “fenced frames”⁷²⁹ included under proposals such as FLEDGE⁷³⁰ could be detrimental from a brand safety perspective. According to Google, “a fenced frame restricts communication with its embedding context to allow the frame access to cross-site data without sharing it with the embedding context”⁷³¹. In practice, this means that publishers do not know what ads were shown to the users visiting their pages, so they are not able to associate the content of this ad with the user. The CMA notes that this could lead to brand safety concerns “by preventing the publisher from knowing what types of ad content is being rendered on its website, and preventing the advertiser from knowing on which publisher inventory its ad content is being placed”⁷³². Ads could be placed next to harmful content, disinformation or content that is simply not brand safe without advertisers’ knowledge.

5.2.2.7 Browsers in control of publisher revenue

As mentioned above, ad delivery under local profiling models happens within the browser, rather than on the publisher’s interface or through their intermediaries. This means that the browser is effectively in control of how or whether publishers are remunerated. Concerns have therefore been raised about the extent to which the Privacy Sandbox proposals will affect publisher revenue. Similarly, it is not clear how much revenue publishers can derive from Brave.

Privacy Sandbox and Brave both entail the blocking of third-party data sharing which, on its own, has potentially significant revenue implications for publishers. Analysis conducted by Google in 2019 suggests that blocking third-party data

⁷²⁸ Publishers and content creators (e.g. on YouTube, Twitch, etc.) can be tipped by users if they sign up to the Creators program. ‘Brave Rewards’ (*Brave*) <<https://creators.brave.com/>>.

⁷²⁹ ‘Fenced Frames’ (*GitHub*) <<https://github.com/WICG/fenced-frame>>.

⁷³⁰ See section 5.2.2.3.1.

⁷³¹ Jack J and others, ‘Fenced Frames’ (*Chrome Developers*, 7 March 2022) <<https://developer.chrome.com/docs/privacy-sandbox/fenced-frame/>>.

⁷³² ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972’ (*CMA*, 11 February 2022) <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

sharing without introducing alternatives to the current digital advertising model would lead the world's top 500 publishers to lose 50% of their ad revenue on average, with some losing over 75%⁷³³. Analysis by the CMA suggests that publishers could see a 70% decline in revenue per impression⁷³⁴. Google has suggested that Privacy Sandbox proposals could alleviate these concerns, and that Google aims to "[support] the ability of publishers to generate revenue from advertising inventory and the ability of advertisers to secure value for money from advertising spend"⁷³⁵.

As mentioned in section 5.2.2.6, concerns have been raised that blocking third-party data sharing could decrease the effectiveness of the intermediary services provided by companies other than Google. This would effectively place limits on the extent to which publishers can use intermediaries and measurement data to prove the value of their services to advertisers. According to two publishers interviewed as part of this study, this could increase publishers' and advertisers' reliance on Google's services⁷³⁶, with one arguing that Google will create "workarounds" to third-party tracking "that only work for them and potentially their clients"⁷³⁷. This could ultimately reduce publishers' choices within the digital advertising supply chain, which could have impacts on their revenues. Additionally, as noted by the CMA, fenced frames "may limit the ability of publishers to control, measure, and optimise content on their websites"⁷³⁸. This could limit publishers' ability to ensure their websites are designed in ways that maximise ad revenue (e.g. by making it more difficult to determine the ad placements that are most conducive to views and clicks). Additionally, the CMA has raised concerns regarding potential conflicts of interest, where Google could self-preference "its own ad inventory and ad tech services via Chrome's decisions on which ads to display to a given web user"⁷³⁹. Respondents to the CMA's consultation highlighted that this would mean that Google could "[interfere] with

⁷³³ Ravichandran D and others, 'Effect of disabling third-party cookies on publisher revenue' (*Google*, 27 August 2019) <https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf>.

⁷³⁴ 'Appendix F: the role of data in digital advertising' in 'Online Platforms and Digital Advertising - Market Study Final Report' (*CMA*, 2020), p. F31 <[https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix F - role of data in digital advertising v.4 WEB.pdf](https://assets.publishing.service.gov.uk/media/5fe495438fa8f56af97b1e6c/Appendix_F_-_role_of_data_in_digital_advertising_v.4_WEB.pdf)>.

⁷³⁵ Malcolm W, 'The path forward with the Privacy Sandbox' (*Google Blog*, 11 February 2022), <<https://blog.google/around-the-globe/google-europe/path-forward-privacy-sandbox/>>.

⁷³⁶ Publishers 3 and 5.

⁷³⁷ Publisher 5.

⁷³⁸ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022), p. 39 <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

⁷³⁹ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022), p. 45 <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

rival publishers' choice to effectively monetize their inventory"⁷⁴⁰. For example, commentators have questioned whether all SSPs will be treated equally in auctions under FLEDGE⁷⁴¹. Indeed, some industry figures have questioned Google's lack of clarity as to how much control it will have over the auction process. Services such as Google Ad Manager have already come under fire for allegedly prioritising Google's own demand, over header bidding⁷⁴².

Google has agreed to commitments to the CMA in an effort to alleviate concerns about potential conflicts of interest. The "non-discrimination" commitment states that Google will not design or implement the Privacy Sandbox proposals in such a way as to "distort competition by self-preferencing Google's advertising products and services"⁷⁴³. As with the other commitments, the CMA will play a role in overseeing Google's compliance. In the event that Google fails to respond to concerns raised by the CMA within 21 days, it may take action pursuant to section 31B(4) Competition Act 1998. Whether this mechanism, along with Google's commitment to refrain from self-preferencing, will actually act as a deterrent against anti-competitive practices remains to be seen. However, the "strengthening [of] restrictions on how Google cannot self-preference" has been commended as a positive step by Mozilla⁷⁴⁴. Nonetheless, the Brave web standards development team has criticised the CMA's commitments in this area for not going far enough, noting that Google has not made a "commitment to not use data learned from Google operating in a first-party context on non-Google sites (e.g. information learned by serving web users AMP pages, information learned from the wide range of data-collecting features included in Chrome, information learned from YouTube and Google Map embeds etc.) to 'improve' ads Google places on Google sites". Their concern is that this could allow Google to "create a moat against competitors"⁷⁴⁵.

Nevertheless, it is worth mentioning claims that some Privacy Sandbox proposals could make it easier for publishers to monetise their platforms and their audiences.

⁷⁴⁰ 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals: Case number 50972' (*CMA*, 11 February 2022), p. 78.

⁷⁴¹ Shields R, 'Google plots further Privacy Sandbox trials but concerns still linger' (*Digiday*, 1 April 2022) <<https://digiday.com/media/google-plots-further-privacy-sandbox-trials-but-concerns-still-linger/>>.

⁷⁴² Włodarczyk L, 'When It Comes To Header Bidding, Will Google Play Fair With FLEDGE?' (*AdExchanger*, 27 April 2022) <<https://www.adexchanger.com/the-sell-sider/when-it-comes-to-header-bidding-will-google-play-fair-with-fledge/>>.

⁷⁴³ 'Competition and Markets Authority Case 50972 - Privacy Sandbox Google Commitments Offer' (*CMA*, 4 February 2022) <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf>.

⁷⁴⁴ "Despite improvements, delaying the deprecation of third party cookies in the CMA's Privacy Sandbox commitments will hold back privacy on the open web" (*Mozilla Blog*, 17 December 2021) <<https://blog.mozilla.org/netpolicy/2021/12/17/privacy-sandbox-cma-dec2021/>>.

⁷⁴⁵ 'Privacy And Competition Concerns with Google's Privacy Sandbox' (*Brave*, 26 January 2022) <<https://brave.com/web-standards-at-brave/6-privacy-sandbox-concerns/>>.

For example, under FLEDGE, publishers could use first-party data to create interest groups relevant to their readership⁷⁴⁶. Google has suggested that publishers “may be able to charge for the ability to show ads to specific segments of their audience” using these interest groups. The revenue impacts of such a proposal are currently unclear.

The way publishers can generate revenues through Brave Ads differs significantly from those proposed under Privacy Sandbox. The Brave browser operates a rewards program (Brave Rewards) to remunerate publishers. This sees publishers and content creators remunerated by users, either in the form of tips disbursed as users browse the web, or on an automatic or active basis (e.g. when a user decides to send BATs to a publisher they particularly like). Additionally, the Brave browser includes an ad blocker which blocks all ads by default⁷⁴⁷. That means that the Creators program is the only way for publishers to generate advertising revenues from the users that access their website using Brave. To this day, the Creators program has 1.5 million content creators signed up, about 120,000 of which are websites, the rest being content creators on platforms such as YouTube, Twitch and Twitter⁷⁴⁸. In practice, it is not clear how much revenue publishers can generate through Brave rewards, or whether this is comparable to revenues they would generate under the current digital advertising model. Brave plans to evolve its approach so as to allow publishers that are part of the Creators program to host ads directly on their websites, enabling them to receive 70% of the spending associated with individual ads⁷⁴⁹.

5.2.2.8 Easier to implement than current model of targeting based on profiling

Local profiling models see advertisers and publishers having a more direct relationship with the browser in question, as blocking third-party sharing would reduce the number of intermediaries involved in ad delivery. This suggests that local profiling models could be easier for publishers and advertisers to use than the current digital advertising model, which could increase their attractiveness to SMEs.

For publishers, generating revenues through local profiling models is as straightforward as the processes defined by the browser, which is the primary intermediary between publishers and users. In the case of Brave Ads, the only

⁷⁴⁶ Dutton S, ‘FLEDGE API’ (*Chrome Developers*, 27 January 2022) <<https://developer.chrome.com/docs/privacy-sandbox/fledge/>>.

⁷⁴⁷ ‘Brave Shields’ (*Brave*) <<https://brave.com/shields/>>.

⁷⁴⁸ ‘BraveBat Home Page’ (*Brave Bat*) <<https://bravebat.info/>>.

⁷⁴⁹ ‘Brave Launches the First Advertising Platform Built on Privacy’ (*Brave*, 24 April 2019) <<https://brave.com/brave-ads-launch/>>.

step at this stage involves joining the Brave Creators program. For advertisers, a direct relationship with the browser is also possible, as is indeed the case with Brave Ads.

5.2.2.9 Unclear impact on pricing

The ways in which local profiling models differ from the current digital advertising model makes pricing comparisons difficult. Additionally, given that Privacy Sandbox has not been implemented yet, it is not clear whether its proposals will come with a price difference for publishers and advertisers compared to the current digital advertising model. In practice, the information that is publicly available does not allow a definite assessment of the price difference between local profiling models and the current digital advertising models.

5.2.3 Popularity of local profiling models

As the technology currently stands, Brave is the only major provider of the local profiling model. On a monthly basis, 50.2 million people use Brave⁷⁵⁰⁷⁵¹. It is active almost 200 countries and has delivered ads from close to 900 advertisers. The EU Member States where the most campaigns have been hosted at any one time are Germany (63 campaigns in January 2022)⁷⁵², the Netherlands (49 in December 2021)⁷⁵³, Italy (47 in January 2022)⁷⁵⁴, Ireland (47 in January 2022)⁷⁵⁵, France (45 in December 2021)⁷⁵⁶ and Denmark (44 in January 2022)⁷⁵⁷. Considering that on average, at least 26% of EU businesses use digital advertising⁷⁵⁸, it appears that Brave Ads has not been widely adopted in the EU.

⁷⁵⁰ 'Brave Passes 50 Million Monthly Active Users, Growing 2x for the Fifth Year in a Row' (*Brave*, 5 January 2022) <<https://brave.com/2021-recap/>>.

⁷⁵¹ 'Brave Passes 50 Million Monthly Active Users, Growing 2x for the Fifth Year in a Row' (*Brave*, 5 January 2022) <<https://brave.com/2021-recap/>>.

⁷⁵² 'Brave Active Ads Campaigns in Germany' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=Germany>.

⁷⁵³ 'Brave Active Ads Campaigns in Netherlands' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=Netherlands>.

⁷⁵⁴ 'Brave Active Ads Campaigns in Italy' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=Italy>.

⁷⁵⁵ 'Brave Active Ads Campaigns in Ireland' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=Ireland>.

⁷⁵⁶ 'Brave Active Ads Campaigns in France' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=France>.

⁷⁵⁷ 'Brave Active Ads Campaigns in Denmark' (*BraveBat*)

<https://bravebat.info/brave_ads_campaigns?country=Denmark>.

⁷⁵⁸ 'Internet advertising of businesses - statistics on usage of ads' (*Eurostat*, December 2018)

<https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads#General_overview>.

As mentioned above, Google's Privacy Sandbox proposals are not currently available in the market. Google plans to "phase out" third-party tracking on Chrome in 2024 with testing for the majority of proposals currently under way⁷⁵⁹. An initial transition period planned in Q3 2023 will see all proposals launched, and a second transition period in Q3 2024 will see third-party data sharing phased out over a two-month period.

5.3 Other emerging digital advertising proposals

This section will provide a short overview of emerging digital advertising tools that are currently under development in digital advertising. These could be used either in combination with the current digital advertising model or with certain alternative models, depending on their nature.

5.3.1 Description

5.3.1.1 Anonymisation, obfuscation and encryption methods

Rendering data anonymous is a useful way of ensuring users' privacy. Under the GDPR, anonymous data is defined as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"⁷⁶⁰. When data is anonymised, it is not considered personal data and, as such, the GDPR does not apply⁷⁶¹, making anonymisation an attractive method in the context of digital advertising. Several new methods of rendering personal data anonymous or quasi-anonymous have been developed:

- **K-anonymity:** this involves masking or removing personally identifiable information, or quasi-identifiers such as IP address. K-anonymity involves generalising individual records, allowing them to be placed in homogenous groups where specific users are indistinguishable from one another. It can be vulnerable to homogeneity attacks and other issues. Accordingly, more

⁷⁵⁹ 'Privacy Sandbox for the Web' (*Privacy Sandbox*) <https://privacysandbox.com/intl/en_us/open-web/>; 'Expanding testing for the Privacy Sandbox for the Web' (*Google Blog*) <<https://blog.google/products/chrome/update-testing-privacy-sandbox-web/>>.

⁷⁶⁰ Recital 26 of the *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1, <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

⁷⁶¹ See Recital 26 GDPR.

complex rules such as l-diversity and t-closeness have been developed. This sort of generalisation was proposed by models such as Privad⁷⁶², in which the user profile is generalised before being sent to an ad broker when requesting ad, and as part of Topics API.

- **Differential privacy:** this involves the introduction of statistical noise or randomness (i.e. random values) within a dataset so as to obfuscate the output. In a digital advertising context, this could involve adding random values (e.g. interests or personal characteristics) to a user profile when it is shared as part of targeting based on profiling, to make it more difficult for the intermediaries that receive the profile to match it with their datasets and re-identify the user in question⁷⁶³. Differential privacy has been used in the past by Meta⁷⁶⁴ and Apple⁷⁶⁵.
- **Cryptography:** various cryptographic methods have been proposed with application to digital advertising, including private information retrieval⁷⁶⁶, zero knowledge proofs⁷⁶⁷, homomorphic encryption⁷⁶⁸ and MPC⁷⁶⁹. These all have the purpose of enabling data processing for digital advertising without revealing the identity of users to third parties in the supply chain.

5.3.1.2 Interoperable Private Attribution

Interoperable Private Attribution (IPA) is a proposal spearheaded by Meta and Mozilla for measuring attribution (i.e. which ad or set of ads can be attributed to

⁷⁶² Guha S, Cheng B and Francis P, 'Privad: Practical Privacy in Online Advertising' (*Proceedings of 8th Symposium on Networked Systems Design and Implementation*, March 2011)

<<https://www.usenix.org/conference/nsdi11/privad-practical-privacy-online-advertising>>.

⁷⁶³ Seufert EB, 'What is differential privacy in digital advertising?' (*Mobile Dev Memo*, 5 April 2021)

<<https://mobiledevmemo.com/what-is-differential-privacy/>>.

⁷⁶⁴ Nayak C, 'New privacy-protected Facebook data for independent research on social media's impact on democracy' (*Facebook Research*, 12 February 2020)

<<https://research.facebook.com/blog/2020/02/new-privacy-protected-facebook-data-for-independent-research-on-social-medias-impact-on-democracy/>>.

⁷⁶⁵ 'Differential Privacy' (*Apple*)

<https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf>.

⁷⁶⁶ Ullah I and others, 'Enabling Privacy Preserving Mobile Advertising via Private Information Retrieval' (*IEEE 42nd Conference on Local Computer Networks*, 2017)

<https://www.researchgate.net/publication/321120831_Enabling_Privacy_Preserving_Mobile_Advertising_via_Private_Information_Retrieval>.

⁷⁶⁷ See Brave's THEMIS proposal: 'Themis' (*GitHub*) <<https://github.com/cossacklabs/themis>>

⁷⁶⁸ See the Adnostic proposal: Toubiana V and others, 'Adnostic: Privacy Preserving Targeted Advertising' (*Cryptography*, December 2010) <<https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf>>.

⁷⁶⁹ Juels A, 'Targeted Advertising... And Privacy Too' (*Lecture Notes in Computer Science*, 2 April 2020)

<<http://www.arijuels.com/wp-content/uploads/2013/09/J01.pdf>>.

a customers' purchasing decision) without tracking⁷⁷⁰. Under IPA, a "match key" is used to tie different browsing events together. This match key is written to the browser by websites and platforms that users log in to, but can only be read by the browser or operating system. Although the match key is tied to the user login, it is only used to tie source events (e.g. impressions and clicks) with trigger events (e.g. product purchases) and is not shared with advertisers or publishers. Instead, the browser bundles events and match keys, and transfers them to semi-trusted servers, to be encrypted using multi-party computation and homomorphic encryption (see section 5.3.1.1). The browser then makes periodic queries to these semi-trusted servers for attribution results. Relegating the matching of events to semi-trusted servers means that the browsers would not have all the user data and encryption keys, and would therefore not be able to identify users based on this information.

5.3.1.3 PARAKEET

Private and Anonymized Requests for Ads that Keep Efficacy and Enhance Transparency (PARAKEET) is a proposal put forward by Microsoft⁷⁷¹. Under PARAKEET, the browser anonymises ad requests to ensure that personal data is not shared with third parties as part of ad delivery. This would see the browser modify ad requests in a variety of ways (e.g. anonymising the context provided by the publisher and anonymising geographic information) to prevent third parties from re-identifying users. Similar to Google's Topics API proposal, the browser uses anonymised user interest categories as the basis for ad targeting. PARAKEET supports the use of retargeting, lookalike targeting (i.e. targeting based on a user's similarity to an advertiser's existing customers) and contextual targeting.

5.3.1.4 MaCAW

Multi-party Computation of Ads on the Web (MaCAW) is another proposal put forward by Microsoft⁷⁷². MaCAW is intended to work together with proposals such as PARAKEET to enable brand safety checks without jeopardising user privacy. As mentioned in section 5.3.1.3, PARAKEET prevents user re-identification by anonymising certain information in bid requests, including publisher contexts. Similar to FLEDGE, MaCAW involves the use of trusted servers to run brand safety models, which enables advertisers to ensure and verify that their ads were placed

⁷⁷⁰ Thomson M, 'Privacy Preserving Attribution for Advertising' (*Mozilla Blog*, 8 February 2022) <<https://blog.mozilla.org/en/mozilla/privacy-preserving-attribution-for-advertising/>>; Titone T, 'Interoperable Private Attribution (IPA) Explained' (*Ad Tech Explained*, 28 February 2022) <<https://adtechexplained.com/interoperable-private-attribution-ipa-explained/>>.

⁷⁷¹ 'PARAKEET' (*GitHub*) <<https://github.com/microsoft/PARAKEYET>>.

⁷⁷² 'MaCAW' (*GitHub*) <<https://github.com/WICG/privacy-preserving-ads/blob/main/MACAW.md>>.

according to their brand safety preferences without identifiers being shared with intermediaries.

5.3.1.5 SPARROW

Secure Private Advertising Remotely Run On Webserver (SPARROW)⁷⁷³, put forward by Criteo, is a proposal to enhance the interest-group targeting that underlies proposals such as Topics API^{774, 775}. Along with the introduction of more advertiser campaign controls (e.g. over campaign budgets, attribution methods, measurement and brand safety), SPARROW's key innovation is a proposal to undertake ad auctions in a third-party trusted server, named the "Gatekeeper", rather than in browser, as is currently proposed in Topics API. This Gatekeeper would be an "internet-based service responsible [for running] interest group auctions and [generating] ad web bundles, instead of the browser". Just like in Topics API, the use of interest categories within the targeting mechanism ensures that personal data is not shared with third parties. That said, just like Topics API, SPARROW would naturally involve profiling and the use of sensitive data by the browser, as well as allowing the use of contextual targeting in combination with targeting based on interest categories.

The proposal has been criticised for its assumption that a third party would necessarily be better placed to protect both user and advertiser data, especially given the limited number of companies with the capacity to undertake the foreseen tasks. As Ari Paparo, CEO of Beeswax, a digital advertising intermediary, pointed out, the conflicts of interest inherent to Topics API⁷⁷⁶ would still remain. "If you made a list of all the companies that could do it, they almost all have ad divisions – cloud companies, telcos, Google, Facebook – who is not conflicted in doing this?"⁷⁷⁷

⁷⁷³ 'SPARROW' (*GitHub*) <<https://github.com/WICG/sparrow>>.

⁷⁷⁴ Topics API and SPARROW are both based on Google's initial Two Uncorrelated Requests, Then Locally-Executed Decision On Victory ("TURTLEDOVE") proposal, which introduced the concept of targeting on the basis of interest categories defined and processed at browser level. See: "TURTLEDOVE" (*GitHub*) <<https://github.com/WICG/turtledove>>.

⁷⁷⁵ See section 5.2.2.3.1.

⁷⁷⁶ See section 5.2.2.3.1.

⁷⁷⁷ O'Reilly L, 'WTF is Dovekey' (*Digiday*, 28 September 2020) <<https://digiday.com/media/wtf-what-is-dovekey>>.

5.3.1.6 PARRROT

Publisher Auction Responsibility Retention Revision of TURTLEDOVE (PARRROT)⁷⁷⁸, proposed by Magnite, is similar to SPARROW in that it builds on the interest-group targeting underlying Topics API⁷⁷⁹. Rather than have ad auctions take place either within a trusted server or within the browser, PARRROT proposes ad auctions take place on the publisher side of the supply chain. PARRROT essentially seeks to replicate header bidding, whereby publishers can make bid requests to multiple SSPs. The use of fenced frames⁷⁸⁰ would prevent the publisher from learning about the contents of the ad, and consequently a user's interests. Like Topics API, PARRROT would allow the use of contextual targeting in combination with targeting based on interest categories.

5.3.1.7 Zero-party data

Zero-party data is generally described as data that is collected directly from users on a voluntary basis. Currently, zero-party data is primarily collected directly by advertisers in the course of their direct relationships with their customers, typically through quizzes and questionnaires⁷⁸¹. This personal data can then be used in targeting and customer research, just like other types of personal data. In theory, zero-party data is more accurate than first-, second- and -third-party data, because it is provided directly by users and can often be quite specific.

As it currently stands, zero-party data is not collected or used in ways that differ from the current digital advertising model. For example, although there are several organisations developing personal information management systems (PIMS) that enable individuals to store and manage access to their personal data⁷⁸², these are not currently used in the digital advertising context. As such, although it possible to imagine a situation where users voluntarily provide their personal data to PIMS that regulate access to that data according to users' preferences, this is not currently a solution that is available.

⁷⁷⁸ 'PARRROT: The Publisher Auction Responsibility Retention Revision of TurtleDove' (*GitHub*) <<https://github.com/prebid/identity-gatekeeper/blob/master/proposals/PARRROT.md>>.

⁷⁷⁹ See footnote 774.

⁷⁸⁰ See section 5.2.2.6.

⁷⁸¹ 'What is Zero-Party Data?' (*Salesforce*) <<https://www.salesforce.com/resources/articles/what-is-zero-party-data/>>.

⁷⁸² See, for example, Solid <<https://solidproject.org/>>.

5.3.2 Evaluation

5.3.2.1 Use of personal data

Although the proposals described in this section are all separate, they all involve restrictions on the use of personal data compared to the current digital advertising model.

5.3.2.1.1 Monitoring and profiling

Like Google's proposal for Topics API, proposals such as PARAKEET, SPARROW and PARRROT all operate on the basis of targeting based on interest groups defined by the browser. The browser in question would associate these interests to users by building profiles of users' interests based on their browsing behaviour. As such, although the data in question would not be shared with third parties, profiling and monitoring are key to their functioning.

5.3.2.1.2 Sensitive data

Similar to Google's Topics API proposal, it is highly likely that browsers would continue to collect users' special category data as part of the monitoring and profiling underlying the PARAKEET, SPARROW and PARRROT proposals. Similarly, zero-party data models could also involve the collection of special category data, with the added benefit that users would have additional control over whether it is shared or not, including for advertising purposes.

Article 26 DSA introduces a prohibition on providers of online platforms to present on their interfaces advertising "based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679"⁷⁸³. This would not prevent browsers from collecting special category data, but could restrict the use of this data for ad targeting purposes in some cases. However, as discussed further in section 7, Google and Facebook already claim to restrict the use of "sensitive interest categories" in "personalised ads"⁷⁸⁴ (Google) and "detailed targeting options that relate to topics people may perceive as sensitive" (Meta)⁷⁸⁵. Some civil society stakeholders consulted for this study have also raised concerns that the wording of Article 26.3 DSA is not sufficiently precise to prohibit non-special category data

⁷⁸³ Article 26.3 of the Digital Services Act. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁷⁸⁴ 'Personalized Advertising' (*Google Support*) <<https://support.google.com/adspolicy/answer/143465?hl=en>> accessed 9 September 2022.

⁷⁸⁵ 'Updates to Detailed Targeting' (*Meta Business Help Centre*) <<https://www.facebook.com/business/help/458835214668072>>.

from being combined and inferred to create new targeting options which could be considered sensitive, for example targeting individuals based on an interest in certain topics known to be linked – albeit not explicitly – to areas such as sexual orientation, religion or health.

5.3.2.1.3 Third-party data sharing

All the emerging tools discussed in this section (except for zero-party data) are being developed in the wake of Google’s Privacy Sandbox initiative and, as such, are designed to operate without sharing personal data with a large number of third parties.

That said, IPA, MaCAW, SPARROW and PARRROT would all rely on the use of trusted servers to operate. They can therefore be said to involve sharing personal data with at least one third party, though the intention is for trusted servers to be able to provide adequate safeguards, including encryption, to ensure that personal data is not shared further.

Whether zero-party data models involve the sharing of personal data with third parties depends on the safeguards put in place by the provider. For example, both in the case of personal data collected via surveys and in the context of PIMS, to ensure that users cannot be re-identified, data might be shared only in aggregated forms, or in an encrypted fashion.

5.4 Subscriptions

Many publishers have explored subscription models as another way of generating revenue beyond advertising. Shifting to an entirely subscription-based model could reduce the need to rely on personal data and profiling to generate digital advertising revenue, although it is unclear how viable this would be for all publishers, especially SMEs. Concerns have also been raised that putting all high-quality independent journalism behind a paywall could have a negative impact on access to information and democracy.

Often associated with the proliferation of paywalls across the internet in recent years, the subscription model is growing in popularity as an alternative means of content monetisation for publishers. In simple terms, subscription models see publishers provide access to their content (or sometimes only certain content) in exchange for a regular fee. The subscription model has found popularity with news publishers looking to offset the decline in digital advertising revenue over the past

20 years⁷⁸⁶. Notable examples include BILD, which had nearly 600,000 BILDplus subscribers as of February 2022⁷⁸⁷, and El País, which acquired over 143,000 digital subscribers in the first 21 months of rolling out its new subscription model⁷⁸⁸. Aside from funding digital journalism, subscriptions also act as an important revenue source for video on demand, also known as subscription video on demand (SVOD), such as Netflix, music streaming services, software companies and independent content creators (often through intermediaries such as Patreon).

However, as will be set out in greater depth, subscriptions have not been universally successful among publishers. Some have suggested subscriptions can be off-putting for consumers who only want access to a particular piece of content, or who are reluctant to make the potentially expensive commitment of purchasing a full subscription. Micropayments, which are small transactions that allow users to access a specific piece of content, have been suggested as a comparable alternative to subscriptions as they could enable users to pay specifically for the content they want to access while being less financially exclusionary to low-income users. Thus, when considering the viability of the subscription model it is important to consider whether micropayments could work alongside, or as an alternative to, subscriptions in helping overcome the barriers to adoption.

5.4.1 Evaluation

5.4.1.1 Use of personal data

The mechanism that underlies the subscription model, periodic payment for access to content, requires neither the monitoring and profiling of users nor the processing and storage of their sensitive personal information (outside of a payment context). Accordingly, the subscription model can use less personal data than ad-based models for funding digital content. However, data can play a role in digital subscription strategies, for instance in the context of dynamic paywalls. Publications such as the Wall Street Journal can use data to assess a user's propensity to subscribe to the publication and thereby determine how many articles a user may access before introducing the paywall⁷⁸⁹. In Europe, Schibsted

⁷⁸⁶ See section 2.4 and 'Newspapers Fact Sheet: State of the News Media' (*Pew Research Centre*, 29 June 2021) <<https://www.pewresearch.org/journalism/fact-sheet/newspapers/>>.

⁷⁸⁷ 'Axel Springer invites media companies to the 9th "International Paid Content Summit"' (*Axel Springer*, 16 February 2022) <<https://www.axelspringer.com/en/ax-press-release/axel-springer-invites-media-companies-to-the-9th-international-paid-content-summit>>.

⁷⁸⁸ 'EL PAÍS surpasses 180,000 subscriptions' (*Prisa*, 7 February 2022) <<https://www.prisa.com/en/noticias/notas-de-prensa/el-pais-supera-los-180.000-suscriptores>>.

⁷⁸⁹ 'The WSJ dynamic paywall' (*International News Media Association*) <<https://s3.amazonaws.com/inma-awards-uploads/8CBFBC944E55939F5C2008DE93DDA5E5.pdf>>.

has experimented with a “semi-dynamic” or “hybrid” paywall wherein “an algorithm tries to identify ‘engaging content’, which will then be put behind the paywall by the newsroom”⁷⁹⁰. Although this does not personalise content to specific users⁷⁹¹, Schibsted has also developed a model to “identify visitors who are three to five times more likely to subscribe”, and then show them different offers to other users⁷⁹².

5.4.1.2 No evidence of impact on advertisers

As a revenue model independent from digital advertising, the subscription model has little interaction with ads, and therefore does not materially impact advertiser-specific issues. For advertisers, perhaps the most significant effect of widespread adoption of the model by publishers, in lieu of funding content through digital advertising or an increase in consumer willingness to purchase subscriptions, would be for their reach to somewhat diminish. Digital subscriptions often involve access to premium content that is free of ads, meaning advertisers would find it more difficult to reach subscribers than users browsing free content. That said, as discussed further in section 5.4.2, the number of publishers funding their content through subscriptions is small, suggesting that subscriptions are currently not a barrier to the growth of digital advertising revenues.

5.4.1.3 A stable source of income with fewer intermediary costs

With some publishers struggling to stay profitable from ad revenue alone, many are drawn to the subscription model as a more sustainable alternative source of income. Generally, fewer intermediary costs are involved when compared with the digital ad supply chain. Unlike with digital ads, where estimates suggest that 50-60% of ad spend is lost to intermediaries and fraud⁷⁹³, publishers typically receive all of the money paid by subscribers. Small content creators might accept payment through an intermediary such as Patreon, but even these sites typically only charge 5-20% of a creator’s monthly subscription income as their fee⁷⁹⁴, which is considerably less than the ad revenue lost to fraud and various intermediaries in

⁷⁹⁰ Leitner M, ‘How media companies use data to sign up digital subscribers (and keep them)’ (*Reuters Institute*, 2018) <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-05/How_media_companies_use_data.pdf>.

⁷⁹¹ Leitner M, ‘How media companies use data to sign up digital subscribers (and keep them)’ (*Reuters Institute*, 2018) <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-05/How_media_companies_use_data.pdf>.

⁷⁹² ‘Reader Revenue: Success stories from the front’ (*Innovation Media*, 16 September 2019) <<https://innovation.media/magazines/new-revenue-streams/case-studies-of-reader-revenue-success-in-digital-media>>.

⁷⁹³ See section 4.3. ‘Guide to Programmatic Media (2014)’ (*World Federation of Advertisers*, 3 July 2014) <<https://wfanet.org/knowledge/item/2014/07/03/Guide-to-Programmatic-Media-2014>>; ‘ISBA Programmatic Supply Chain Transparency Study’ (*ISBA*, 2020) <<https://www.isba.org.uk/system/files/media/documents/2020-12/executive-summary-programmatic-supply-chain-transparency-study.pdf>>.

⁷⁹⁴ ‘Pricing’ (*Patreon*) <<https://www.patreon.com/en-GB/pricing-page-en>>.

the supply chain. Digital subscriptions also have the potential advantage of being relatively predictable. Publishers have relatively precise data about their total number of subscribers and know, in turn, how much revenue to expect will be generated on a regular basis.

5.4.1.4 Difficult to scale, especially for SMEs

While the model has provided a reliable source of revenue for some major publishers, smaller publishers have faced greater obstacles in pivoting towards digital subscriptions. Large publishers benefit from widespread brand recognition and greater resources to reach potential subscribers through advertising. In some cases, large publishers may have access to more extensive digital infrastructure which could result in a better user experience on their digital properties. By contrast, SME publishers and small content creators tend to have a smaller pool of potential subscribers as their content might be specific to a local area, or catered to a particular community or niche interest group. This is supported empirically by research by the Reuters Institute which found that the majority of subscriptions worldwide go to “just a few big national brands”⁷⁹⁵, and that the dynamic of the model can be characterised as “winner takes most”⁷⁹⁶. In a time of rising living costs, publications with a low-income readership might also struggle to persuade readers to purchase a costly subscription. As a result, 47% of publishers are concerned that “subscription models may be pushing journalism towards superserving richer and more educated audiences and leaving others behind”⁷⁹⁷. Faced with the choice between small, local or niche publishers, who might publish a handful of articles daily, and a large international publication offering access to different topics, games and dozens of new articles each day, most consumers will opt for the latter. Of the small publishers interviewed by this study, only one was primarily subscriptions-funded⁷⁹⁸, while the other two derived the majority of their revenues from advertising⁷⁹⁹.

As discussed in section 4.1.1, this issue is exacerbated by suggestions that “subscription fatigue” could see users become increasingly frustrated by the fragmentation of content across multiple services. Additionally, there is evidence to suggest that consumers are tiring of managing the multiple subscriptions

⁷⁹⁵ Newman N, ‘Overview and Key Findings of the 2021 Digital News Report’ (*Reuters Institute*, 23 June 2021) <<https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/dnr-executive-summary>> accessed 8 May 2022.

⁷⁹⁶ Newman N and others, ‘Digital News Report 2021’ (*Reuters Institute*, 2021), p. 14 <[https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital News Report 2021 FINAL.pdf](https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital%20News%20Report%202021%20FINAL.pdf)>.

⁷⁹⁷ Newman N, ‘Journalism, Media, and Technology Trends and Predictions 2022’ (*Reuters Institute*, 10 January 2022), p. 6 <<https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-01/Newman%20-%20Trends%20and%20Predictions%202022%20FINAL.pdf>>.

⁷⁹⁸ Publisher 7.

⁷⁹⁹ Publishers 4 and 8.

acquired during COVID-19. In Q1 2022, 1.5 million subscribers cancelled their streaming subscriptions, which, as Alistair Gray suggested in the *Financial Times*, could be because “viewers have become more discerning about subscribing to multiple platforms”⁸⁰⁰.

Indeed, an important obstacle to the growth of digital subscriptions is that many consumers are unwilling to pay for certain types of content such as news. The Reuters Institute suggests that this is because “most people are not interested enough in news, or do not have sufficient disposable income to prioritise news over other parts of their life”, resulting in a mere 17% of consumers across 20 countries having paid for online news in the 12 months preceding February 2021⁸⁰¹. Some users may also have an entrenched perception of certain types of content as “free”, having become accustomed to free access funded by digital advertising or other sources of funding (e.g. state-funded media). Indeed, one small publisher went so far as to argue that their local readers “in general are not willing to pay for content”⁸⁰².

5.4.1.5 A barrier to access to quality content

Concerns have also been raised about the subscription model creating barriers to accessing important information online, which could see high-quality independent journalism limited to a relatively small subset of the population who are willing and able to pay the subscription fees. A situation wherein disinformation is widely available on free-to-access sites (potentially funded by malicious actors) while the reputable sources required to rebut the disinformation are locked behind paywalls could undermine the extent to which the electorate are able to make informed decisions on social and economic issues, to the detriment of democracy⁸⁰³. The impact of widespread pay-walling could even undermine access to online tutorials and e-learning materials, which have acted as important educational resources for individuals from low-income backgrounds.

5.4.1.6 Innovation could partially remedy subscription fatigue

While the subscription model has clear limitations, these issues could potentially be mitigated or remedied through policy and model design choices. Content aggregation services allow users to view articles from multiple publishers in one feed, while not having to switch between websites to manage payments. If

⁸⁰⁰ Gray A, ‘UK households cancel streaming subscriptions in record numbers’ (*Financial Times*, 18 April 2022) <<https://www.ft.com/content/1c7e255e-a537-40e4-9dd7-6061175ba5f3>>.

⁸⁰¹ Newman N and others, ‘Reuters Institute Digital News Report 2021’ (*Reuters Institute*, 2021), p. 14 <[https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital News Report 2021 FINAL.pdf](https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital%20News%20Report%202021_FINAL.pdf)>.

⁸⁰² Publisher 4.

⁸⁰³ Pickard V, ‘Salvation Or Folly?: The Promises and Perils of Digital Paywalls’ (2014) 2 *Digital Journalism* p. 212, <https://repository.upenn.edu/cgi/viewcontent.cgi?article=1439&context=asc_papers>.

aggregators allow consumers to feel less “fatigued” than managing multiple news subscriptions, they could play a role in diminishing the “winner takes most” dynamic that favours large publishers. To address concerns about pay-walling and access to trustworthy information online, some have suggested that governments could subsidise or cover the cost of news outlet subscriptions. An example of such a proposal is the Local Journalism Sustainability Act in the US, which proposes offering the public a tax credit of up to \$250 to cover 80% of the cost of a local newspaper subscription⁸⁰⁴. Aside from increasing local publisher revenues, a public journalism allowance could promote equal access to journalism.

Micropayments have struggled to see broad adoption among publishers, despite their initial popularity in early discussions on the future of the digital economy. Some have suggested that a deeper issue with the model is that consumers are less willing to repeatedly undergo the process of paying for individual pieces of content compared to paying for access on a monthly or yearly basis. Each request for payment heightens the “pain of paying” for consumers, a sense of discomfort at having to consider the financial cost of a publisher’s content⁸⁰⁵. Combined with the disruption to user experience caused by repeated requests for payment, micropayments face a number of barriers that have hampered their widespread adoption. These issues are exemplified by the switch of one of the most high-profile micropayment services, Blendle, to subscriptions, because they provided “much more stable” revenue⁸⁰⁶. Broadly, the key issue for publishers with using micropayments is likely to be unpredictable income and the high volume of transactions required to generate significant revenues.

Similarly to digital subscriptions, several innovations have been suggested as methods to increase the viability of microtransactions for publishers. A unified digital wallet to enable micropayments seamlessly across different sites, without disruption or constant prompting, could alleviate concerns about the “mental transaction cost” for consumers. Some have also suggested that the low transaction costs of certain cryptocurrencies could make payments that are “worth fractions of a cent”⁸⁰⁷ financially viable for publishers. A micropayment of this size

⁸⁰⁴ "H.R.3940 - 117th Congress (2021-2022): Local Journalism Sustainability Act" *Congress.gov*, Library of Congress, 16 June 2021, <<https://www.congress.gov/bill/117th-congress/house-bill/3940/all-info?r=1&s=1>>.

⁸⁰⁵ Ahearn A, ‘A Behavioral Economist Breaks Down The Pain of Paying’ (*Acumen Academy*) <<https://www.acumenacademy.org/blog/pain-paying/>> accessed 11 June 2022.

⁸⁰⁶ Schmidt C, ‘Micropayments-for-News Pioneer Blendle Is Pivoting from Micropayments’ (*Nieman Lab*, 10 June 2019) <<https://www.niemanlab.org/2019/06/micropayments-for-news-pioneer-blendle-is-pivoting-from-micropayments/>> accessed 22 May 2022.

⁸⁰⁷ Klein M and Stummer C, ‘Feeless Micropayments as Drivers for New Business Models: Two Exemplary Application Cases’ (*Frontiers in Blockchain*, 18 March 2021) <<https://www.frontiersin.org/articles/10.3389/fbloc.2021.641508/full>>.

to stream a song or read an article would involve little financial risk and could perhaps be less off-putting to consumers.

5.4.2 Popularity of the subscription model

The adoption rate of the subscription model varies heavily based on the nature of the publisher, with some sectors, such as SVOD services, being entirely funded by subscriptions and others, such as individual content creators, being more difficult to gauge. Data from 2019 suggests that 46% of leading newspapers in the EU countries sampled used paywalls⁸⁰⁸, with this figure likely having risen in the subscription “boom” during the COVID-19 pandemic⁸⁰⁹. Additionally, research from the Reuters Institute found that 79% of publishers surveyed worldwide considered “subscription and membership strategies” to be one of their most important revenue priorities for 2022, “ahead of both display and native advertising”⁸¹⁰. Estimates as to the revenue share of advertising and digital subscriptions vary, but subscriptions may now constitute a higher share of revenue for news outlets than advertising⁸¹¹. But US survey data from 2020 suggests that the “breakdown of subscription revenue vs. advertising revenue” was that 72% of revenue for publishers came from advertising and the remaining 28% came from subscriptions⁸¹². Broadly, digital advertising retains the largest share of publisher revenue, but revenue from subscriptions appears to be growing for some types of content⁸¹³. This suggests that although subscriptions remain an important revenue source for publishers, the model may increasingly be used in combination with digital advertising.

⁸⁰⁸ Simon FM and Graves L, ‘Pay Models for Online News in the US and Europe: 2019 Update’ (*Reuters Institute*, May 2019), p. 3 <[https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-05/Paymodels for Online News FINAL 1.pdf](https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-05/Paymodels%20for%20Online%20News%20FINAL%201.pdf)>.

⁸⁰⁹ Turvill W, ‘Media subscription trends report: After the Covid-19 boom, how can publishers persuade readers to continue paying for news?’ (*PressGazette*, 6 May 2021) <<https://pressgazette.co.uk/media-subscription-trends-report-piano/>>.

⁸¹⁰ Newman N, ‘Journalism, Media, and Technology Trends and Predictions 2022’ (*Reuters Institute*, 10 January 2022) <<https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-01/Newman%20-%20Trends%20and%20Predictions%202022%20FINAL.pdf>>.

⁸¹¹ Based on figures from publicly traded newspapers in the US. See: ‘Trends and Facts on Newspapers | State of the News Media’ (*Pew Research Center’s Journalism Project*, 29 June 2021) <<https://www.pewresearch.org/journalism/fact-sheet/newspapers/>> accessed 1 May 2022.

⁸¹² ‘Combined Revenue Models Gaining Traction in Media Industry’ (*Lineup*, November 2021) <<https://lineup.com/wp-content/uploads/2021/11/English-Combined-Revenue-Models-Gaining-Traction-in-Media-Industry.pdf>>.

⁸¹³ With the caveat that some writers are suggesting the market has reached “peak subscription”. See: Mull A, ‘This Is Peak Subscription’ (*The Atlantic*, 3 March 2022) <<https://www.theatlantic.com/health/archive/2022/03/why-subscriptions-are-hard-to-cancel/623885/>>.

Alongside direct subscriptions to specific publications, some services aggregate content from multiple publishers on a single platform. The most popular news aggregators are free-to-use services owned by major platforms, such as Apple News, Facebook News, MSN and Google News. MSN⁸¹⁴ and Apple News⁸¹⁵ alone respectively have approximately 550 million and 125 million monthly users globally. Most of these services are ad-funded, with the benefit for publishers typically coming from increased traffic (and consequently ad revenue), licensing fees, and direct payment from the aggregator. Some services are subscription-based, with users paying monthly fees for access to articles, and though not as ubiquitous as free-to-access platforms, some services such as Apple News+ are seeing considerable growth. By one estimate, micropayments have not seen widespread adoption in the context of digital content, however start-ups such as Dropp and Helium (both based in the US) suggest the model could see a return to relevance⁸¹⁶.

5.5 Key findings

This section considered two alternative digital advertising models currently available or in development, as well as other emerging digital advertising tools: contextual advertising and local profiling models (including Google's Privacy Sandbox). It also considered subscriptions as an important method of revenue generation for publishers. Each model was evaluated with regards to whether it involves (a) the monitoring of individual behaviour and the profiling of individuals, (b) the processing of special categories of data, as defined by Article 9 GDPR (also referred to as "sensitive personal data") and (c) the sharing of personal data with multiple third parties. The impact of each model on publishers and advertisers was evaluated according to the issues respondents described in section 4, including barriers to (or incentives for) adoption. This section's findings were considered in relation to the current regulatory framework (e.g. the GDPR) and proposed instruments (e.g. the DSA and the DMA).

Key findings

Alternative models can rely on less personal data. Of the models considered, contextual advertising appears to be the model that relies on the least personal

⁸¹⁴ Mandhana T, '550 million monthly readers. 180 countries. 31 languages. And \$1B in sustainable revenue returned to the news industry since 2014' (*MSN Blogs*, 7 October 2020) <<https://blogs.msn.com/microsoft-news-1b-revenue-partners/>>.

⁸¹⁵ Matney L, 'Apple News sites 125 million monthly active users' (*TechCrunch*, 30 April 2020) <<https://techcrunch.com/2020/04/30/apple-news-hits-125-million-monthly-active-users/>>.

⁸¹⁶ Birch D, 'New Ledgers, New Business Models And New Opportunities In Micropayments' (*Forbes*, 30 April 2022) <<https://www.forbes.com/sites/davidbirch/2022/04/30/new-ledgers-new-business-models-and-new-opportunities-in-micropayments/>>.

data. If used without identifiers, contextual advertising can be done in a way that does not rely on monitoring and profiling individuals, the use of special category data, or sharing personal data with multiple third parties. Local profiling models on the other hand do involve the monitoring and profiling of individuals and could also involve the processing of special category data. That said, like contextual models, local profiling models can entail the blocking of third-party data sharing.

It is unclear whether alternative models are effective in comparison to the current digital advertising model. The availability of evidence on the effectiveness of contextual advertising and local profiling models is limited. Although case studies and research by providers of the models suggest their use could have benefits in comparison with the current digital advertising model, the amount of independent research is limited. This could make it more difficult for advertisers and publishers to justify investing in alternative models.

Local profiling models (such as the one in development by Google) see browsers in control of key elements of digital advertising. This includes the definition of targeting criteria, the data available on the effectiveness of campaigns, the extent to which publishers are remunerated, and the controls available for preventing ads from appearing alongside disinformation and harmful content. This could limit advertisers' and publishers' ability to make choices. Additionally, when it comes to publisher revenues, concerns have been raised about Google's potential conflicts of interest.

Alternative models generate less data to measure the effectiveness of campaigns. Table 9 provides an overview of the measurement data available when using contextual advertising or local profiling models. Google has indicated that all categories of measurement data will remain available under the Privacy Sandbox proposals, albeit in a more limited fashion. As described in section 4, this is a key concern for advertisers, as well as for publishers who fear it could limit their ability to prove the value of their ad inventory.

The targeting capabilities of alternative models are more limited. Because contextual advertising does not rely on personal data, advertisers' options for targeting using contextual advertising are more limited than the targeting options currently available. That said, the technology is evolving to develop more sophisticated targeting techniques using new technologies. Advertisers have similarly raised concerns about the more limited targeting criteria involved under local profiling models such as Google's Privacy Sandbox. Concerns have also been raised about the control that Google would have over the creation and maintenance of the targeting taxonomy.

Evidence of the impact of alternative models on publisher revenues is limited. It is therefore unclear whether contextual advertising and local profiling models are sufficient to alleviate the potential revenue shock associated with turning off third-party data sharing.

Alternative models could involve fewer intermediaries than the current digital advertising model. The restrictions that both models place on the use of personal data means that both contextual advertising and local profiling models could involve the use of fewer intermediaries. This could reduce costs and complexity, both of which are common issues raised by advertisers and publishers in relation to the current model.

Few advertisers and publishers are currently using alternative models. Both contextual advertising and local profiling are relatively new models that have not yet been widely adopted. That said, once implemented, Google's Privacy Sandbox proposals could become one of the most widely used digital advertising models as a result of Google's reach and position.

Other emerging privacy tools are currently in development which could contribute to reducing the amount of personal data used in digital advertising. That said, while proposals such as PARAKEET, SPARROW and PARRROT would place limits on third-party data sharing, they would likely still involve the monitoring and profiling of users and the use of special category data.

Subscriptions are an imperfect alternative to digital advertising revenues. Although subscriptions present a privacy-friendly way for publishers to generate revenues, publishers' ability to scale subscriptions depends on their size. Although new tools are being developed which could encourage subscription-related revenues (like micropayments and news aggregators), evidence of the effectiveness of these tools is still limited. Subscriptions nonetheless represent an important source of revenue for publishers, though this may often be in combination with digital advertising revenues.

Current digital advertising model	Contextual advertising	Local profiling models (excl. Privacy Sandbox)	Privacy Sandbox
Impressions Viewability Reach Frequency Engagement Conversions	Impressions Viewability Engagement (clicks only)	Impressions Viewability Engagement Conversions	Impressions Viewability Reach Frequency Engagement Conversions

Table 9: Overview of the measurement data that can be generated in campaigns using the current digital advertising model and alternative models.

6 Ways for individuals to indicate their preferences for data collection and targeting

Individuals don't have adequate control over how their personal data is collected and used for digital advertising. Although several industry tools exist which claim to enable individuals to review and control how their data is used for the most widely used types of digital advertising, our assessment suggests that most are not user-friendly and deploy a multitude of design features and language choices that undermine the ability of users to exercise control over their own data. These deficiencies are compounded by the fact that individuals are required to indicate their preferences across all of these tools separately in order to influence the way that ads are targeted to them across all the devices, apps and sites they use.

6.1 Introduction

This section will consider the extent to which user-friendly and convenient ways exist for individuals, including children and young people, to indicate their preferences for data collection and targeting.

In a digital advertising context, there are several ways in which individuals can indicate their preferences for data collection and ad targeting. As outlined in section 1.3.1, digital advertising today relies on large amounts data collected by a range of different companies (including large platforms, intermediaries, publishers and advertisers), using various methods for a variety of different purposes. As a result, a fragmented and complex data landscape has emerged. A patchwork of regulation, self-regulation and voluntary actions by industry stakeholders has provided individuals with a limited number of tools to indicate their preferences within different parts of this complex data landscape. Most of these efforts fall short of providing meaningful user-friendly and convenient options for individuals.

There is a wealth of research from various disciplines into the mechanics of practices such as "dark patterns", "deceptive design" and "nudges". Some studies have suggested that dark patterns are prevalent within data preference tools used

in digital advertising⁸¹⁷. Dark patterns can be used to guide users to select the option that allows the most data collection, sharing and processing in the context of digital advertising⁸¹⁸. Studies that assess the compliance of data preference tools with data protection legislation highlight the importance of their design⁸¹⁹. As well as influencing choices, the way the architecture and interfaces of data preferences tools are designed can impact individuals' autonomy and control⁸²⁰.

In the context of the current EU regulatory framework, focus often shifts to the way that individuals provide consent for tracking⁸²¹, though this is only a very limited and blunt form of preference. For example, consent implies giving users the option to say "yes" or "no" to sharing their data, but not necessarily allowing individuals to subsequently control how this data is used to determine what ads they see. This is why the review in this section focuses primarily on tools which allow users to access information about how their data is used for advertising on an ongoing basis and make changes to their preferences, rather than consent mechanisms designed to communicate consumer consent in the context of regulatory compliance.

The General Data Protection Regulation (GDPR) provides for individuals to exercise some control over how their personal data is processed for digital advertising purposes through Article 21.2 GDPR, which provides data subjects with the right

⁸¹⁷ Nouwens M, Liccardi I, Veale M, Karger D, Kagal L, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (CHI '20: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 23 April 2020) <<https://arxiv.org/abs/2001.02479>>.

⁸¹⁸ Nouwens M, Liccardi I, Veale M, Karger D, Kagal L, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (CHI '20: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 23 April 2020) <<https://arxiv.org/abs/2001.02479>>.

⁸¹⁹ See, for example: 'Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy' (Forbrukerrådet, 2018) <<https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>>; Bauer JM, Bergstrøm R and Foss-Madsen R, 'Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data' (2021) 120 *Computers in Human Behavior* <<https://doi.org/10.1016/j.chb.2021.106729>>.

⁸²⁰ Competition and Markets Authority, 'Online Choice Architecture How digital design can harm competition and consumers' (*CMA Discussion Paper*, April 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf>.

⁸²¹ The ePrivacy Directive stipulates consent requirements for using tracking tools like cookies, while the definition of consent is specified in the GDPR. The ePrivacy Regulation, a proposal to revise the ePrivacy Directive, is currently under consideration. 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), OJ L 201, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>; and Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD), <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>>.

to object to the processing of personal data for direct marketing at any time, including profiling. A discussion of the extent to which direct marketing (in this context) corresponds to digital advertising based on profiling is included in section 6.2. Section 6.2 also considers the extent to which this right can be used to provide individuals with user-friendly and convenient ways to indicate their preferences for data collection and targeting in a digital advertising context.

Beyond regulatory requirements, providing transparency, control and choice over how people's data is used for digital advertising is often cited by the industry as essential requirements for a sustainable digital advertising ecosystem. These sentiments are found in the context of industry self-regulation programmes⁸²², public statements related to privacy made by companies⁸²³, privacy notices and cookie banners, and various industry statements, manifestos and commitments⁸²⁴. Although there is no central interface which allows individuals to do this for all types of digital advertising, several voluntary and self-regulatory tools have been designed by the digital advertising industry and specific companies to enable individuals to indicate their preferences to some extent within limited parts of the advertising ecosystem:

- The European Interactive Digital Advertising Alliance (EDAA) manages a self-regulatory initiative called Your Online Choices (YOC) which aims to "foster transparency in the online advertising environment for all, through delivering consumer-facing information and control solutions with regard to how data is used for interest-based advertising"⁸²⁵. This tool offers individuals the option to turn on and off data collection by "some of the providers who work with websites to collect and use information to provide interest-based advertising".
- Google offers an "ad personalisation" interface for logged-in users⁸²⁶ that "make[s] it easy to control the data used to personalise ads to you"⁸²⁷. This

⁸²² 'Home Page' (European Interactive Digital Advertising Alliance) <<https://edaa.eu/>> accessed 19 May 2022.

⁸²³ 'Privacy Policy – Privacy & Terms' (*Google Policies*) <<https://policies.google.com/privacy?hl=en-US>>; Zuckerberg M, 'Starting the Decade by Giving You More Control Over Your Privacy' (*Facebook News*, 28 January 2020) <<https://about.fb.com/news/2020/01/data-privacy-day-2020/>>.

⁸²⁴ 'WFA Manifesto for Online Data Transparency' (*World Federation of Advertisers*, 20 April 2018) <<https://wfanet.org/knowledge/item/2018/04/20/WFA-Manifesto-for-Online-Data-Transparency/>>.

⁸²⁵ 'Your Online Choices' (*European Interactive Digital Advertising Alliance*) <<https://www.youronlinechoices.eu/>> accessed 18 May 2022.

⁸²⁶ This review was carried out in April and May 2022 and refers to the tools which were available during that time period. 'Ad Settings' (Google Ad Settings) <<https://adssettings.google.com/authenticated/>>, accessed 18 May 2022.

⁸²⁷ 'Google Ads Data and Privacy' (*Google Safety Center*) <<https://safety.google/intl/en/privacy/ads-and-data/>> accessed 18 May 2022.

tool offers individuals the option to view different “factors”⁸²⁸ used to target ads to them. Some of these factors can be turned off and others can be updated. Individuals can also turn off all “ad personalisation”. Changes made using this tool apply “anywhere you’re signed in with your Google Account, including on the 2+ million websites and apps that partner with Google to show ads”⁸²⁹.

- Facebook offers an “ad preferences” interface for logged-in users that lets them “view, add and remove preferences that we created for you”⁸³⁰. This tool offers individuals the option to adjust a range of parameters used to target ads to them (for more detail, see section 6.5 below). Changes made using this tool apply “to all the Facebook and Instagram accounts in your Accounts Centre”.

Consumer research carried out in 2022 by a group of digital advertising industry stakeholders (including the European Interactive Digital Advertising Alliance, the World Federation of Advertisers, the European Publishers Council and IAB Europe) concluded that “consumers want to be able to practically, meaningfully and simply curate their own advertising experience when online”⁸³¹. The same study notes that “while [...] such control already exists in principle, many expressed that too often the tools they had at their disposal were not practical enough, either because they had to be fiddled with on each website or because they were different and/or complex to properly understand”.

This section considers the extent to which these tools offer individuals user-friendly and convenient ways to indicate their preferences for data collection and targeting in a digital advertising context.

6.2 The GDPR and the proposed ePrivacy Regulation

The GDPR provides data subjects with the right to object to the processing of personal data for direct marketing at any time, including profiling (Article 21.2 GDPR). This applies to both “initial or further” processing (Recital 70). The proposed ePrivacy Regulation would introduce a harmonised definition of “direct marketing” in EU law. Although the final text has not yet been agreed in trilogue,

⁸²⁸ ‘Ad Settings - Ad Personalization’ (*Google Ad Settings*)

<<https://adssettings.google.com/authenticated>> accessed 19 May 2022.

⁸²⁹ ‘Google Ads Data and Privacy’ (*Google Safety Center*) <<https://safety.google/intl/en/privacy/ads-and-data/>> accessed 18 May 2022.

⁸³⁰ This review was carried out in April and May 2022 and refers to the tools which were available during that time period. ‘Ad Preferences’ (*Facebook Help Centre*)

<<https://www.facebook.com/help/109378269482053>> accessed 19 May 2022.

⁸³¹ ‘Your Online Voices’ (*European Interactive Digital Advertising Alliance*, 2022) <https://edaa.eu/wp-content/uploads/YOV_external-report_27.06.pdf>.

the definitions proposed by the European Commission, the European Parliament and the Council all include references to digital advertising “to one or more identified or identifiable” end-users. Since all types of advertising referenced in section 1 use individuals’ personal data in some form to target ads to them, this definition – and therefore the “right to object” of Article 21.2 GDPR – could apply. In the absence of an agreement on the ePrivacy Regulation, several national data protection authorities (DPAs) have published definitions of direct marketing which, again, could all be understood to extend to the types of digital advertising referenced in section 1 .

The GDPR states that the right to object to data processing for direct marketing must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information” (Article 21.4 GDPR). Article 21.5 GDPR provides for this right to be exercised “by automated means using technical specifications”. Although some of the ad preference tools reviewed below do offer users the ability to “turn off” ads that are targeted to them based on their personal data, our evaluation concludes that the majority of these tools are not easy to access and therefore not “explicitly brought to the attention of the data subject”. In addition, it is not clear to what extent these tools could be considered as an exercise of the rights provided for in Article 21.2 GDPR because there is not sufficient transparency around the actions companies take in response to the use of these tools with regards to data processing.

Further, the right to object in Article 21.2 GDPR has not been subject to regulatory or court action, resulting in questions as to its scope and reach. For instance, it is unclear if the right to object under Article 21.2 GDPR provides a basis for individuals to object to being subject to profiling or allocated interest categories by social media companies entirely, where those social media companies rely on personalised advertising for their business model.

In addition, research has suggested that multiple, possibly hundreds, of separate entities can access advertising data every time a webpage is accessed⁸³². The absence of any centralised mechanism to register objections to processing results in individuals needing to expend significant effort in order to indicate their data collection preferences to all the companies. This issue is aggravated by lack of transparency: information about how data is processed for digital advertising purposes is usually provided in various different documents spread across the different sites and apps that the person uses (e.g. privacy policies, cookie policies and information notices, account settings).

⁸³² ‘The Biggest Data Breach - ICCL Report on the Scale of Real-Time Bidding Data Broadcasts in the U.S and Europe’ (*Irish Council for Civil Liberties*, 16 May 2022) <<https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>>.

The European Commission's proposal for an ePrivacy Regulation⁸³³ included a provision for consent to be expressed using technical settings of a software application enabling access to the internet (e.g. a browser). This would apply to consent required for companies to use processing and storage capabilities of terminal equipment and the collection of information from terminal equipment (e.g. via cookies that collect data for digital advertising purposes, as outlined in section 1.3.1.1). This could complement the right to object to processing outlined above but it may not apply to all cases of data collection linked to digital advertising, such as data collected without the use of cookies or trackers – for example in the context of a first-party relationship between an individual and a company when signing up for an account or subscription. It is also important to note that the industry is increasingly moving away from technologies that involve placing trackers such as cookies on terminal equipment in favour of other forms of identification such as user accounts and email addresses (see section 1.3.1.1.4).

6.3 Industry tools

As outlined in section 1.3.1, digital advertising today relies on large amounts of data collected by a range of different companies (including large platforms, intermediaries, publishers and advertisers) in many different ways. As a result, a fragmented and complex data landscape has emerged. It is important to note that there is currently no single user interface where individuals can see and control all the data that is collected about them for digital advertising purposes by different companies, and how it is used for ad targeting. Instead, different slices of the digital advertising ecosystem make a limited set of options available to individuals in specific contexts. Individuals are expected to navigate the different options and understand how choices made through different user interfaces interact with each other in order to get a global view of how this impacts what ads they are shown on any given app or website. This section will consider to what extent some of these tools offer individuals user-friendly and convenient ways to indicate their preferences for data collection and targeting in a digital advertising context.

⁸³³ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003 (COD) <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications>>.

6.3.1 Choice of tools to review

The two companies which earn the most revenue from digital advertising, Google and Meta, offer specific interfaces where logged-in users of their services can view and, in some cases, exercise limited control over how their data is collected and/or how ads are targeted to them. Given the leading role these two companies play in digital advertising today, we have decided to review Google Ad Settings and Facebook Ad Preferences.

Large amounts of data are also collected about individuals outside of Google and Meta's apps and websites. Beyond Google and Meta, thousands of companies⁸³⁴ use third-party trackers (e.g. cookies, software development kits (SDKs)) to collect data for digital advertising purposes (see section 1.3.1.1) and determine how ads are targeted to individuals. This is most often linked to "other" display advertising (see section 1.1.2.4) which appears on different publisher websites and apps. Individuals who want to indicate their preferences regarding data collection and targeting in this context would, theoretically, need to interact with each company separately using different interfaces or systems. In an effort to centralise these requests, the digital advertising industry launched YOC, a self-regulatory programme, in 2012. YOC is a website that enables individuals to see, on an ongoing basis, a list of the different companies that have collected their data⁸³⁵ and "turn off"⁸³⁶ ad targeting by these companies. This section will review the YOC interface.

Finally, on mobile devices, a large amount of data collection is controlled by the operating system (OS) of the device. There are two main types of OS for mobile devices in Europe: Google's Android (69% of the market) and Apple's iOS (30% of the market)⁸³⁷. Individuals can indicate their preferences regarding data collection and targeting through OS settings, in addition to the options listed above. In 2021, Apple updated the way that individuals are offered choices regarding data collection by third parties, known as App Tracking Transparency (ATT). These changes have attracted a significant amount of attention in the digital advertising industry because they have led to a large drop in the number of people who can be tracked across sites and apps on Apple devices. Given the impact these changes have had on some parts of the digital advertising ecosystem

⁸³⁴ 'The Biggest Data Breach' (*Irish Council for Civil Liberties*, May 2022) <<https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe>>.

⁸³⁵ This is limited to companies that have signed up to participate in the Your Online Choices programme.

⁸³⁶ 'For Consumers' (*European Interactive Digital Advertising Alliance*) <<https://edaa.eu/what-we-do/for-consumers/>> accessed 19 May 2022.

⁸³⁷ See section 1.3.1.1.2.

(for example, Meta forecasted a \$10 billion loss linked to ATT)⁸³⁸, we will review ATT.


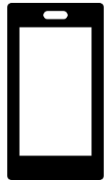
Device	Service	Ad preferences tools
	Google-owned services	Google ad settings
	Meta-owned services	Facebook ad settings
	"Other" display ecosystem (includes Google and Meta as intermediaries)	Your Online Choices
	Google-owned services	Google ad settings
	Meta-owned services	Facebook ad settings
	Mobile device	Ad settings vary depending on phone and OS
	Browser (similar to the "other" display ecosystem above)	Your Online Choices

Table 10: Mapping of the different tools assessed in this section to parts of the digital advertising ecosystem.

For the purposes of this study, we have focused on some of the tools which cover the biggest portions of the digital advertising ecosystem (see table 10). However, it is important to note that even if an individual were to adjust their data collection preferences on all of the interfaces assessed in this section, this would most likely not cover all data collection and targeting practices in the digital advertising ecosystem. As explained above, the fragmented and complex nature of the digital advertising ecosystem makes it difficult – if not impossible – for individuals to exercise complete control over how their data is shared within this network. The Belgian data protection authority, *Autorité de protection des données (APD)*, found that “the large number of third parties i.e. the ad tech vendors that will potentially receive and process the personal data of the users contained in the bid request” meant that real-time bidding (RTB), one of the key delivery methods for “other” display advertising, fails to give individuals sufficient transparency over how their personal data is processed and prevents them from providing informed consent⁸³⁹.

⁸³⁸ Gilbert B, ‘Facebook Blames Apple after a Historically Bad Quarter, Saying iPhone Privacy Changes Will Cost It \$10 Billion’ (*Business Insider*, 3 February 2022) <<https://www.businessinsider.com/facebook-blames-apple-10-billion-loss-ad-privacy-warning-2022-2>> accessed 18 May 2022.

⁸³⁹ Belgian *Autorité de Protection des Données*, ‘Case number: DOS-2019-01377. Complaint relating to Transparency & Consent Framework’ (21 February 2022) <<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>>.

6.3.2 Assessment methodology

This review is based on three factors:

- (i) **Access:** how easy it is for individuals to access the tools, or the place where they can indicate their data collection and targeting preferences. We considered the number of steps needed to access the tool and general visibility.
- (ii) **Comprehension:** how easy it is for individuals to understand the interface and the information presented to them in order to make an informed choice regarding their preferences. We considered the language used (simple or technical) and the amount of information presented.
- (iii) **Action:** how easy it is for individuals to indicate their preferences and use the options provided. We considered usability and the number of actionable steps available to indicate preferences, and whether individuals can turn personalisation on or off at once.

The review took place in April and May 2022 and includes screenshots of the interfaces from that period. It is possible that changes may have been made to these interfaces between May 2022 and publication of this study. To review Google, Facebook and Apple's tools, the accounts of an AWO team member were used. Ads were selected at random, based on a search query of a supermarket brand on Google Search, after watching a video on YouTube's home page, and by scrolling down the home page of the Facebook website and the app. The tools were reviewed in their English language versions.

The scope of this review only relates to the interface presented to individuals. It did not analyse the actual collection of data and ad targeting resulting from the selection of different options.

Interfaces were reviewed by AWO, where possible and where relevant, on both desktop and mobile. Two different scenarios were considered: (1) when individuals want to change their preferences at any time, through settings and (2) when individuals want to change their preferences when looking at an ad.

6.3.3 Findings

Out of the four tools assessed in May 2022, only one can be considered user-friendly. Most tools, even when presenting user-friendly interfaces in terms of language and actionability, have barriers in place preventing easy access.

Table 11 summarises the finding of our review and classifies the tools based on whether they were

- User-friendly ✓
- Somewhat user-friendly ○
- Not user-friendly ✗

	Access	Comprehension	Action	Total
Google Ad Settings	✗	✓	✓	○
Facebook Ad Preferences	✗	○	✗	✗
Your Online Choices	✗	✗	✗	✗
Apple’s App Tracking Transparency	✓	✓	✓	✓

Table 11: Summary of findings of section 6.

Broadly, the findings of the review point to significant deficiencies in the three assessed factors across most of the tools. It is possible that changes may have been made to these interfaces between when the review was carried out in May 2022 and the date of publication of this study.

User-friendly access is a notable issue across three of the four interfaces, with Apple’s consent prompts currently serving as the only tool that is easily accessible to users. By contrast, four steps are needed for a user to access the Google Ad Settings interface for indicating ad preferences. Accessing settings in relation to a particular ad, for instance on a YouTube video, requires clicking on a small button which does not bear clear labelling as to its purpose. Similarly, accessing the interface for indicating data collection and targeting preferences on Facebook requires users to take six steps, and already be aware of which tabs to select. The YOC tool likewise lacks user-friendly accessibility; access generally requires recognition of the YourAdChoices icon.

The comprehensibility of the information presented about users’ choices in the tools evaluated varied greatly. Google Ad Settings uses relatively easy to understand language and features generally succinct explanations. That said, this brevity could undermine the extent to which users are able to make informed choices. Although Facebook Ad Preferences also uses simple language and useful examples of what each setting does, the overall design is unintuitive. Perhaps the least easily comprehensible tool is the YOC interface, which involves technical language, and presents users with a long list of companies collecting personal data. Taken together, these factors could make comprehension of the interface

difficult and overwhelming for users. Apple's ATT uses short sentences and features a simple binary choice of "Ask App Not to Track" or "Allow" that gives users a clear understanding of how to use the interface and the effect of their choice.

Finally, several of the tools reviewed do not make it easy for users to indicate their preferences. The YOC tool suffers from major usability flaws. For one, users are unable to turn off data collection from all companies at once without scrolling through the page and indicating their preference via a pop-up. Additionally, on some browsers, indicating an opt-out preference may have no effect at all. Even after indicating an opt-out preference for all listed companies, the YOC tool will sometimes still show companies as continuing to collect data. Users also face considerable usability issues when interfacing with Facebook Ad preferences. Aside from lacking a single option to turn off all personalisation, the ability to opt out of certain "Ad Topics" is limited to a handful of topics, and users must manually opt out of different "categories used to reach you" to manage their data. The process of turning off ad personalisation through Google settings is comparably straightforward. Users can click on a single button to turn off all personalisation, although specifying more granular preferences about ad targeting through the Ad Settings interface can be time consuming.

On balance, the tools assessed lack user-friendliness to varying extents and feature a multitude of design features and language choices that undermine the ability of users to exercise control over their own data. The simple language and design of certain aspects of the Google Ad Settings interface is offset by confusing design inconsistencies elsewhere, and friction in the user interface that makes accessing the tool difficult. Likewise, issues with access and comprehension in the design of Facebook Ad Preferences make the key settings that are relevant to most users difficult to find. Additionally, the YOC tool for indicating ad preferences suffers from significant defects in usability, accessibility and comprehensibility.

6.4 Google Ad Settings

This review focused on the Google Ad Settings interface which was available to users when the review was carried out in April and May 2022. This "ad personalisation" interface for logged-in users⁸⁴⁰ "make[s] it easy to control the data used to personalise ads to you"⁸⁴¹. This tool offers individuals the option to

⁸⁴⁰ 'Ad Settings - Ad Personalization' (*Google Ad Settings*)

<<https://adssettings.google.com/authenticated?hl=en>> accessed 19 May 2022.

⁸⁴¹ 'Google Ads Data and Privacy' (*Google Safety Center*) <<https://safety.google/intl/en/privacy/ads-and-data/>> accessed 18 May 2022.

view different “factors”⁸⁴² used to target ads to them. Some of these factors can be turned off and others can be updated. Individuals can also turn off all “ad personalisation”. Changes made using this tool apply “anywhere you’re signed in with your Google Account, including on the 2+ million websites and apps that partner with Google to show ads”⁸⁴³.

The tool allows individuals to turn “ad personalisation” on or off. By turning it on, users give Google permission to show ads based on their activity across all Google services and their devices. As users use Google services, or browse websites and apps, the factors used to personalise their ads will be updated and can be deleted or updated in the interface. The interface we used showed 90 factors which could be turned off. Age, gender and language could not be turned off but only updated.

This interface is only available to users who are logged in to a Google account. Non-logged-in users are directed to YOC (section 6.6).

Although there is little published data related to consumer awareness and use of Google’s Ad Settings, a study by Tschantz et al. found that only 5.4% of respondents had opted out of tracking on Google services via Google Ad Settings⁸⁴⁴. By contrast, 70-80% of users have opted out of tracking on devices via Apple’s ATT tool (section 6.7). This significant difference may indicate a lack of consumer awareness and/or difficulties in accessing and using Google Ad Settings. Additionally, the literature does not contain surveys evaluating whether individuals understand Google Ad Settings and the impacts of its different configurations.

6.4.1 Desktop

6.4.1.1 Indicating preferences through settings

6.4.1.1.1 Access

Google Ad Settings are not easy to find: four steps are required to reach the settings interface (click on account icon on the top right corner → then “Manage

⁸⁴² ‘Ad Settings - Ad Personalization’ (*Google Ad Settings*)

<<https://adssettings.google.com/authenticated?hl=en>> accessed 19 May 2022.

⁸⁴³ ‘Google Ads Data and Privacy’ (*Google Safety Center*) <<https://safety.google/intl/en/privacy/ads-and-data/>> accessed 18 May 2022.

⁸⁴⁴ It is important to note that though this paper was published in 2018, the survey data is from 2014. The Google Ad Settings interface has since changed, and the opt-in rates may have changed since research was conducted. Tschantz MC and others, ‘The Accuracy of the Demographic Inferences Shown on Google’s Ad Settings’ (*arXiv*, 22 August 2018) <<http://arxiv.org/abs/1808.07549>> accessed 19 May 2022.

your Google Account” → then “Data & Privacy” → then scroll down to find and click on “Ad settings”). Users must know which tab to select to access the page, as advertising is not mentioned in the tab titles or in the main page. When individuals want to change their preferences, it is also possible that users may confuse the Google Ad Settings associated with their account with the privacy settings associated with Google Chrome.

6.4.1.1.2 Comprehension

The language used is fairly easy to understand as there are only a few short sentences of explanation. However, this limited information can also be a barrier to making an informed choice. The information does not mention data collection and instead focuses on how Google uses data to make advertising more “useful”.

6.4.1.1.3 Action

It is easy to turn ad personalisation on and off with one click (see figure 7). However, indicating more granular preferences regarding ad targeting is time-consuming and burdensome. The interface provides a long list of interests which must be manually selected and then turned off, and the categories of age, gender and language can only be updated and not turned off.

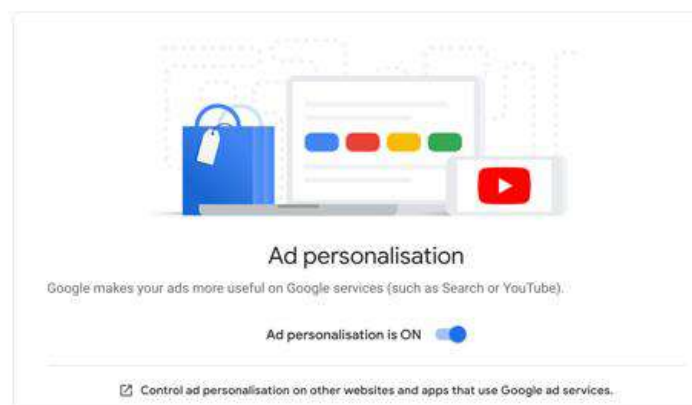


Figure 7: Google Ad Settings (May 2022)⁸⁴⁵.

6.4.1.2 When individuals see an ad

Ads reviewed included Google Search ads and YouTube ads (ads embedded in a YouTube video – video or banners, ads accompanying video ads displayed outside the video, and ads in the video feed).

⁸⁴⁵ 'Ad Settings - Ad Personalization' (*Google Ad Settings*)

<<https://adssettings.google.com/authenticated?hl=en>> accessed 3 May 2022.

6.4.1.2.1 Access

The button to access information on the ad or to change settings is difficult to access and fairly hard to find. On Google Search ads (see figure 8), the icon button is a small triangle which does not inform the individual of its purpose and is easily overlooked.



Figure 8: A Google Search ad (May 2022)⁸⁴⁶.

Not all YouTube ads have the same icons, which can be confusing for users. Ads embedded in a YouTube video (video or banners) and ads accompanying video ads displayed outside the video use the same icon (see figure 9). This icon indicates that more information might be found there, but it does not indicate that settings can be changed. Ads displayed in the video feed have a different icon (three dots, see figure 9), which also does not necessarily inform the individual of the possibility to indicate preferences.

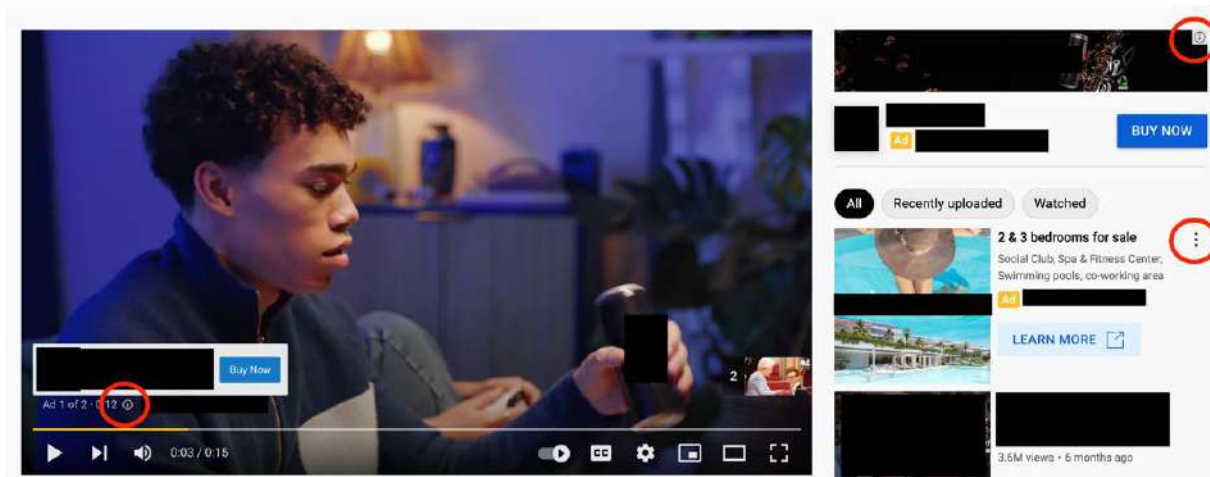


Figure 9: Three types of ads on YouTube with their respective icons highlighted (May 2022)⁸⁴⁷.

⁸⁴⁶ Page result after typing the name of a supermarket brand on Google Search <<https://google.com>> accessed 5 May 2022.

⁸⁴⁷ Video (YouTube) <<https://www.youtube.com/watch?v=l0Xw6NMIQ4>> accessed 6 May 2022.

On both Google ads and YouTube ads, clicking on the icon button leads to an almost identical pop-up window where individuals can then easily reach the Google Ad Settings page (see figure 10). However, clicking on the three dots icon on YouTube ads does not directly lead to the pop-window but to a pop-up banner first (see figure 11). Individuals must then click on “Why this ad?” to access the pop-up window which leads to the settings.

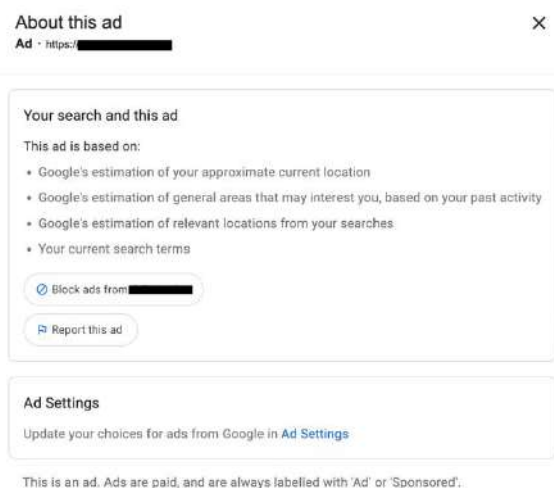


Figure 10: Google Search pop-up window (May 2022)⁸⁴⁸.

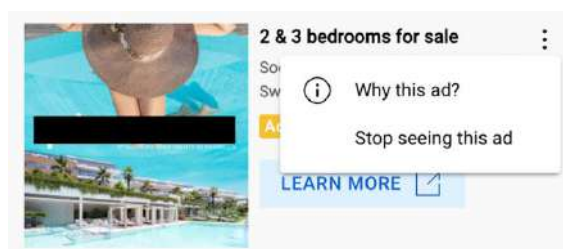


Figure 11: YouTube pop-up banner after clicking on the three dots icon (May 2022)⁸⁴⁹.

Overall, it is difficult for individuals to access settings as the buttons are small, quite hidden and it is not obvious that these buttons allow them to change their preferences regarding data collection and ad targeting.

6.4.1.2.2 Comprehension

The pop-up window (figure 10) is quite user-friendly as the language used is short, concise and simple to understand. This window leads to the Google Ad Settings interface (see section 6.4.1.1).

The pop-up banner (figure 11) does not clearly indicate that ad settings or data collection preferences can be changed by individuals.

6.4.1.2.3 Action

The pop-up window leads to the Google Ad Settings interface (see section 6.4.1.1).

⁸⁴⁸ Page result after typing the name of a supermarket brand on Google Search <<https://google.com>> accessed 5 May 2022.

⁸⁴⁹ Video (*YouTube*) <<https://www.youtube.com/watch?v=l0Xw6NMIRQ4>> accessed 6 May 2022.

6.4.2 On mobile

6.4.2.1 Indicating preferences through settings

6.4.2.1.1 Access

Individuals can access their Google account settings on any of the Google suite of apps. As with the desktop version, it is not easy to find (see section 6.4.1.1).

Access on the YouTube app is inconsistent with access on desktop as the settings tabs have different titles. The link to the Google Account settings from the “Ad settings” section opens a new window within the app for the user to sign into their Google account, which is not convenient and can deter individuals.

6.4.2.1.2 Comprehension

The same language is used as in the desktop version (see section 6.4.1.1).

6.4.2.1.3 Action

It is as easy on mobile as with the desktop version (see section 6.4.1.1).

6.4.2.2 When individuals see an ad

6.4.2.2.1 Access

The button to access information and to change preferences for Google Search ads is not consistent with the desktop version (three dots icon, see figure 12). The same pop-window as on the desktop version appears (see figure 10).



Figure 12: A Google Search ad on mobile (May 2022)⁸⁵⁰.

⁸⁵⁰ Page result after typing the name of a supermarket brand on Google Search <<https://google.com>> accessed 3 May 2022.

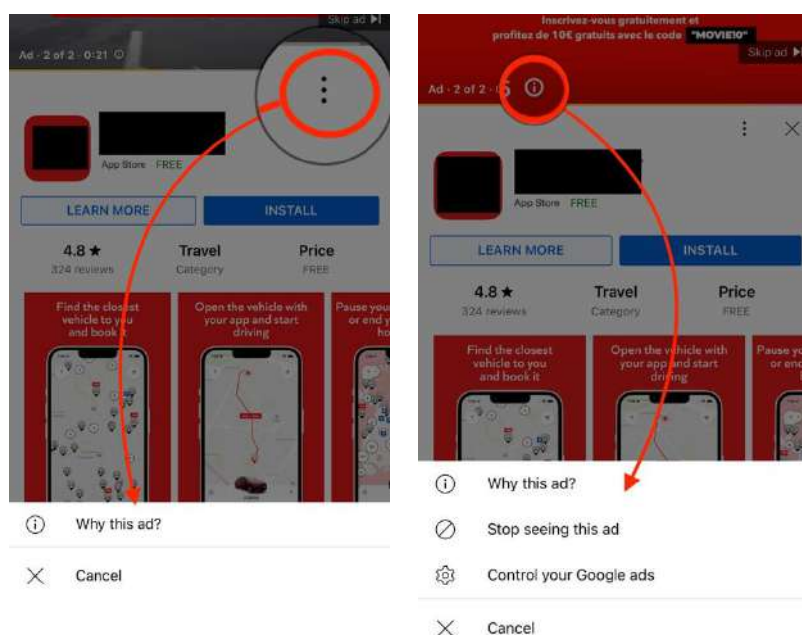


Figure 13: The different icons and pop-up banners associated with a single ad on the YouTube app (May 2022)⁸⁵¹.

For YouTube ads, as with the desktop version, the icons vary depending on where the ad is placed on the page. Additionally, the icons associated with ads in the YouTube app are not consistent with the icons on desktop. The purpose of these inconsistencies is not clear from a functionality standpoint.

The icon associated with ads embedded into videos (e.g. pre-roll ads) is the same both on the YouTube app and on desktop. For all other ads, whether they are part of the feed or accompany the ad in the video, the icon is different (three dots icon, see figure 13). Moreover, the pop-up banners vary in content depending on which button the individual clicks. For ads embedded in videos and ads in the feed, the first pop-up banner contains a direct link to the Google account settings. Conversely, for ads accompanying video ads, a pop-up banner appears before individuals can reach the pop-up window with a link to change settings. It should be noted that, as seen above, the link provided does not lead to the in-app YouTube settings where individuals could change settings. Instead, the app requires users to sign into their Google account, which acts as an additional and potentially inconvenient step.

For all types of ads on the YouTube app, the buttons are small, hard to find and it is not obvious that these buttons allow individuals to change their preferences regarding data collection and ad targeting. This makes it difficult for users to access their ad settings on the YouTube app.

⁸⁵¹ YouTube app, accessed 6 May 2022.

6.4.2.2.2 Comprehension

On Google Search, the pop-up window that appears on mobile is the same as on desktop. This is also the case for the window that appears after clicking the “Why this ad?” banner on YouTube (see figures 10 and 11).

For YouTube ads embedded in videos (see figure 13) the “Why this ad?” banner can be confusing for users who want to change their settings as the wording does not clearly indicate that settings can be changed. “Why this ad?” merely suggests an explanation of why a user is seeing an ad, rather than an opportunity to change ad settings. This contrast is evident when looking at the other ad settings banner associated with ads embedded in videos, which has a specific button for settings (see figure 13). This latter banner is easier to understand and indicates a clear way to change preferences.

6.4.2.2.3 Action

Once on the Google account settings, it is as easy as with the desktop version (see section 6.4.1.1).

6.4.3 Conclusion

The Google Ad Settings interface is not a user-friendly way of indicating data collection and targeting preferences. The tool is quite user-friendly in terms of design and language, except for the interests list which is not convenient to update. On mobile, the information provided and the options to change settings are presented in a user-friendly way in pop-up windows.

However, these positive points are overshadowed by inconsistencies, confusing design choices and complex processes, which strongly impact access and awareness. The design creates excessive and unjustified friction that makes it difficult for individuals to access ad settings. On mobile more specifically, the choice of icons and design inconsistency make the experience more difficult and confusing for individuals. The ambiguity of the icon used on Google Search ads makes it almost impossible for individuals to understand that it can be used to access ad settings.

6.5 Facebook Ad Preferences

This review focused on the Facebook “ad preferences” interface which was available to users when the review was carried out in April and May 2022. Facebook’s “ad preferences” interface for logged-in users lets them “view, add and

remove preferences that we created for you”⁸⁵². This tool offers individuals the option to adjust a range of parameters used to target ads to them (see section 6.5.1.1). Changes made using this tool apply “to all the Facebook and Instagram accounts in your Accounts Centre”.

The interface is composed of three sections titled “Advertisers”, “Ad topics” and “Ad settings”. The “Advertisers” section allows individuals to see the most recent advertisers whose ads they have seen or clicked, and to hide them. In “Ad Topics”, individuals can choose to see fewer ads about a limited number of topics (alcohol, parenting, pets, social issues, elections or politics). The “Ad settings” page has a small Q&A part at the top with two questions, and then allows individuals to manage their data under four different categories (see *Figure 14*):

- **Data about your activity from partners:** where users can choose whether Facebook can use data from their partners to show personalised ads.
- **Categories used to reach you:** where users can choose whether their profile information can be used to show ads and whether advertisers can reach users based on interest categories associated with the user by Facebook.
- **Audience-based advertising:** where users can view advertisers whose audiences they are included in and decide whether this data can be used to show ads.
- **Ads shown off Facebook:** where users can decide whether advertisers can reach them based on categories on websites outside Facebook.

This interface is only available to users who are logged in to a Facebook account. Non-logged-in users are directed to YOC (see section 6.6).

Prior to addressing the extent to which Facebook’s ad preferences are user-friendly, it is important to note that studies have shown that many users may have little awareness of their ability to access this tool at all. Research by Haji and Stock on user awareness of Facebook’s ad settings found that “only about 40% of participating Facebook users know about personalization of settings of their advertising preferences”⁸⁵³. Nonetheless, it is worth noting that the Haji survey covered only young German users, meaning that there is a possibility of generational, regional and/or cultural bias. Its findings are nonetheless comparable with an earlier study undertaken in the US by Pew Research which

⁸⁵² ‘Ad Preferences’ (*Facebook Help Centre*) <<https://www.facebook.com/help/109378269482053>> accessed 19 May 2022.

⁸⁵³ Haji R and Stock WG, ‘User Settings for Advertising Optimization on Facebook: Active Customer Participation or Settings Blindness?’ (2021) 59 *Telematics and Informatics* <<https://linkinghub.elsevier.com/retrieve/pii/S0736585320302070>> accessed 18 May 2022.

found that 74% of US users polled “did not know that Facebook maintained” a “list of their interests and traits”⁸⁵⁴. Nonetheless, neither survey evaluated the degree to which users understood Facebook’s ad preferences and the impacts of its different configurations.

6.5.1 On desktop

6.5.1.1 Indicating preferences through settings

6.5.1.1.1 Access

Facebook Ad Preferences are not easy to find as six steps are required to reach the page where an individual can indicate their data collection and ad targeting preferences: clicking on the triangle icon on the top right -> then “Settings & Privacy” -> then “Privacy Centre” -> then scrolling down to find the “Ads” tab -> then “Review Ad preferences” -> and then selecting the apps concerned. Individuals must already be aware that such preferences can be changed in their Facebook settings, and which tab to select to change these preferences, as advertising is not mentioned early on. As there are multiple categories within the page (see figures 14 and 15), users must complete multiple other steps to indicate their preferences in each category.

6.5.1.1.2 Comprehension

Overall, the language used is clear, fairly easy to understand and the explanation includes easy-to-understand examples. However, the different categories and amount of information in each, as well as the similar language used, can sometimes be confusing for users (see figure 15) and cause information overload. In terms of design, the way the multiple tabs are displayed on the far left of the page and the general design of the page is not intuitive. It does not allow for preferences to be quickly indicated (see figure 14).

⁸⁵⁴ Hitlin P, Rainie L and Olmstead K, ‘Facebook Algorithms and Personal Data’ (*Pew Research Center: Internet, Science & Tech*, 16 January 2019)
<<https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/>>
accessed 18 May 2022.

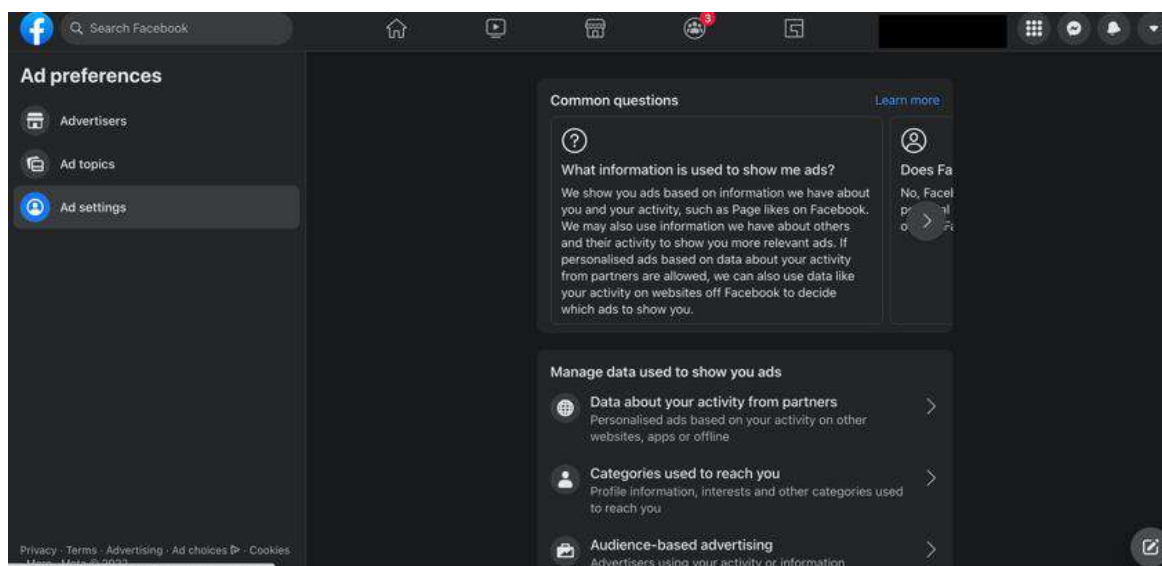


Figure 14: Ad settings page in the Facebook Ad Preferences tool (May 2022)⁸⁵⁵.

6.5.1.1.3 Action

The interface to change Facebook ad settings does not allow individuals to turn personalisation on and off at once. Individuals can only manage their data preferences at the level of “Advertisers”, “Ad topics” and “Ad settings”, and in these categories, there are many paths to many buttons to turn on or off. In the “Advertisers” section, there is no indication of the timeframe over which these ads were seen by the user or whether the list is exhaustive.

In “Ad settings”, there is no option to indicate preferences for all categories at once. In “Data about your activity from partners” and “Ads shown off Facebook section”, users can indicate their preferences with a button, turning the use of data on or off at once. In “Categories used to reach you”, users can only turn four categories on or off with a simple button (employer, job title, education and relationship status) and there is a further list of interests, on another page, which must be edited manually, one at a time. Similarly, in the “Audience-based advertising” section, users must edit the list of businesses one at a time, which can be burdensome as both lists are long.

⁸⁵⁵ ‘Ad Settings’ (Facebook Ad Preferences) <https://www.facebook.com/adpreferences/ad_settings> accessed 3 May 2022.

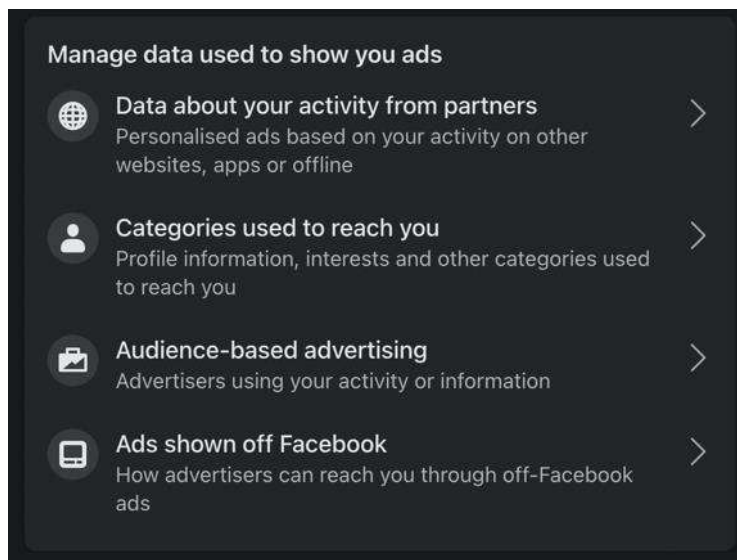


Figure 15: Ad settings page, Facebook Ad preferences (May 2022)⁸⁵⁶.

6.5.1.2 When individuals see an ad

6.5.1.2.1 Access

The button to access the settings is small and the icon does not inform users that it allows them to change their preferences regarding data collection and ad targeting (e.g. in comparison to icons such as gears which are usually used to indicate setting changes, see figure 16). Individuals must then take two other steps to access the ad settings (click on the icon → then “Why am I seeing this ad?” → then “Make Changes to Your Ad Preferences”, see figures 16 and 17).

⁸⁵⁶ ‘Ad Settings’ (Facebook Ad preferences) <https://www.facebook.com/adpreferences/ad_settings> accessed 3 May 2022.

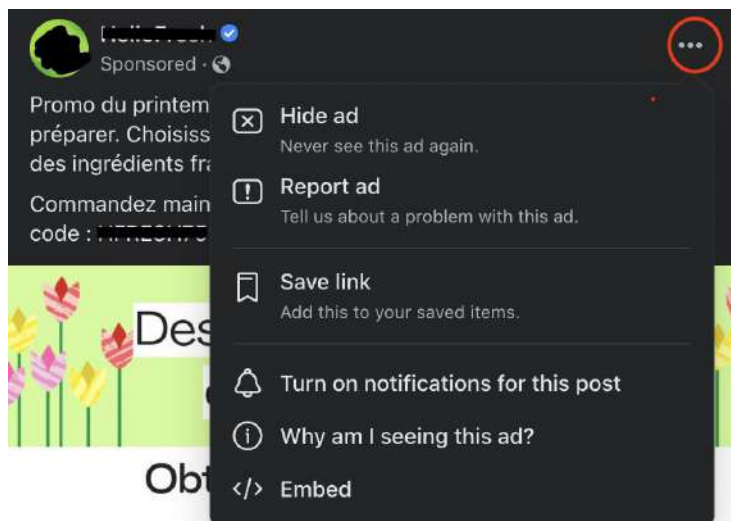


Figure 16: Ad on Facebook, with triple dot icon clicked (May 2022)⁸⁵⁷.

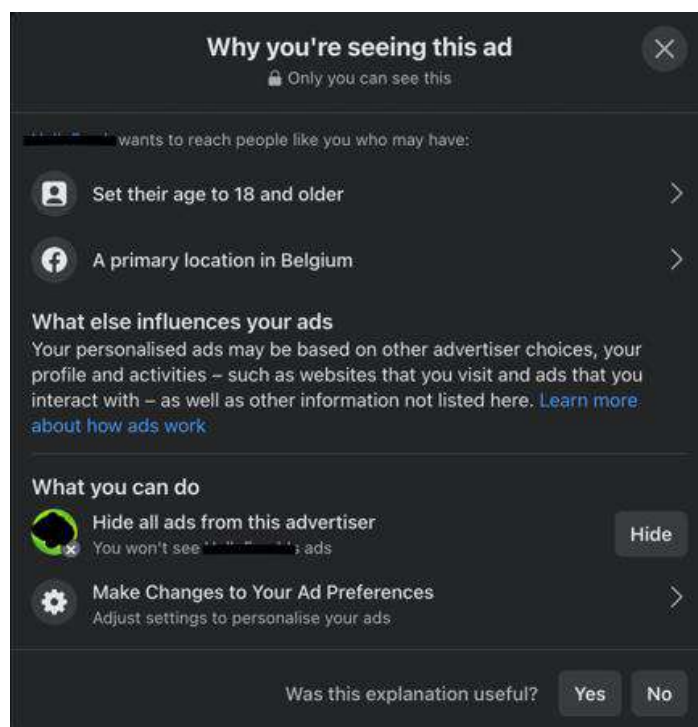


Figure 17: Pop-up window after clicking "Why am I seeing this ad?" on a Facebook ad (May 2022)⁸⁵⁸.

6.5.1.2.2 Comprehension

When the pop-up window appears (figure 16), it is not clear at first glance that individuals can change their ad settings. The second pop-up window is easier to

⁸⁵⁷ 'Home Page' (Facebook) <<https://www.facebook.com/>> accessed 3 May 2022.

⁸⁵⁸ 'Home Page' (Facebook) <<https://www.facebook.com/>> accessed 3 May 2022.

understand *Figure 17* (figure 17). The link leads to the Facebook Ad Preferences interface (see section 6.5.1.1).

6.5.1.2.3 Action

The pop-up window leads to the Facebook Ad Preferences interface (see section 6.5.1.1).

6.5.2 On mobile

6.5.2.1 Indicating preferences through settings

6.5.2.1.1 Access

Access to ad preferences is easier on the app, with three steps instead of six (Click on "Menu" -> then on the gear icon -> then scroll down to the "Permissions" section to click on "Ad preferences"). Although the ad preferences are easier to find on mobile than on desktop as they appear on the main page of the settings, individuals need to understand in which section the page is located and look for it by scrolling through the different sections.

6.5.2.1.2 Comprehension

When looking for the "Ad preferences" settings on the Facebook mobile app, individuals might be confused as the link is not in the "Preferences" section, but in the lower section, "Permissions". The language used on the "Ad preferences" page is fairly easy to understand. The explanation includes easy-to-understand examples.

6.5.2.1.3 Action

The design of the interface is more user-friendly on the Facebook app than on desktop but, similar to the desktop version, the multiple tabs and pages could be confusing for users and there is no option to change settings all at once (see section 6.5.1.1).

6.5.2.2 When individuals see an ad

6.5.2.2.1 Access

The settings button on Facebook mobile ads is big but visually ambiguous as to its purpose (see figure 18). Like the desktop version, it is not clear at first glance

in the pop-up window that individuals can change their ad settings. Individuals must take two further steps to access the setting changes (click on “Why am I seeing this ad?” -> then “Make Changes to Your Ad Preferences”, see figure 19).



Figure 18: Ad on Facebook app (May 2022)⁸⁵⁹.

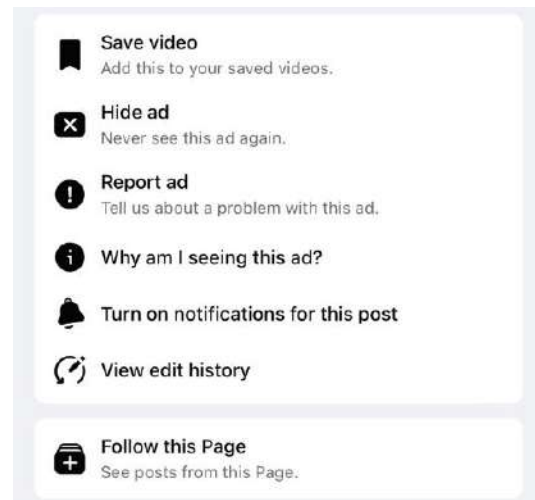
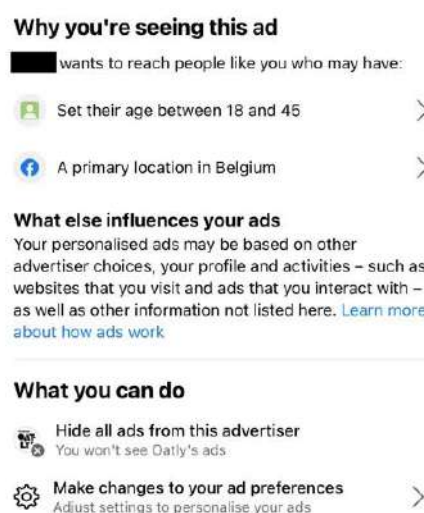


Figure 19: First pop-up window on Facebook app (May 2022)⁸⁶⁰.

6.5.2.2.2 Comprehension

Information on the first pop-up window can be confusing for individuals who want to change their ad settings. The second pop-up window is easier to understand and indicates a clear way to change preferences (see figure 20). The link leads to the Facebook Ad Preferences page (see section 6.5.1.1).



⁸⁵⁹ 'Home Page' (Facebook app) accessed 19 May 2022.

⁸⁶⁰ 'Home Page' (Facebook app) accessed 3 May 2022.

Figure 20: Pop-up window after clicking "Why am I seeing this ad?" on Facebook app⁸⁶¹.

6.5.2.2.3 Action

The pop-up window leads to the Facebook Ads preferences (see section 6.5.1.1).

6.5.3 Conclusion

The Facebook Ad Preferences tool is not a user-friendly way to indicate data collection preferences. Similar to Google Ad Settings, the information displayed and the options to change settings are presented in a user-friendly way in pop-up windows, but access and comprehension is overall difficult. The design creates excessive friction that makes it difficult for individuals to access or navigate the settings. The settings give so much information that the most relevant information and the way to actually indicate preferences is difficult for users to find and assess. On mobile, the design choices, especially icons to access settings, impair access to – and awareness of – the tool.

6.6 The European Interactive Digital Advertising Alliance's Your Online Choices tool

The EDAA manages the self-regulatory initiative Your Online Choices (YOC), which aims to "foster transparency in the online advertising environment for all, through delivering consumer-facing information and control solutions with regard to how data is used for interest-based advertising"⁸⁶². This tool offers individuals the option to turn on and off data collection by "some of the providers who work with websites to collect and use information to provide interest-based advertising".

Through this tool individuals can see a list of companies that collect data about them for digital advertising purposes and select to turn this on or off. This can be done for each company individually or for all companies at once (although there are some limitations to this latter option, see section 6.6.3).

Although recent survey data from the EDAA shows that awareness of the tool is increasing, the percentage of respondents who had seen the AdChoices Icon (without AdMarker) was below 30% in Germany, Spain, Poland, Italy, Sweden,

⁸⁶¹ 'Home page' (*Facebook app*) accessed 6 May 2022.

⁸⁶² 'Your Online Choices' (*European Interactive Digital Advertising Alliance*) <<https://www.youronlinechoices.eu/>> accessed 18 May 2022.

Belgium and France⁸⁶³. Across these countries, the engagement rate (percentage who had clicked on the icon) among the individuals who did recognise the icon ranged between 42% and 56%. Unfortunately, the literature does not contain independent research to confirm the EDAA's findings, and the EDAA did not seek to evaluate the degree to which surveyed users understood the YOC tool and the impacts of its different configurations.

6.6.1 Access

The tool can be accessed from different sources. The most common point of access encountered during this review was when seeing a display ad served on publisher websites and apps. Most frequently, this happened via ads placed by Google, given that Google's ad network served most of the ads encountered during this review. YOC can also be accessed through Google account settings for logged-in users as an additional option to "control ads from other ad networks" (see figure 21) and for non-logged-in users as an option to "opt out of more ads". Non-logged-in users who try to access the Facebook settings referred to in section 6.5.1.1 are directed to YOC as a way to "manage online interest-based ads". Individuals can also directly access the website, youronlinechoices.eu.

From the Google account settings, YOC is easily accessible through a link below the button to turn personalisation on or off. When users turn personalisation off, a pop-up window informs them of the option to turn off ad personalisation through YOC as well (see figure 21). Individuals can also scroll all the way down to find the link to access the tool at the bottom of the page, although this placement is less visible to users (see figure 21).

⁸⁶³ France: 21%, Italy: 27%, Spain: 27%, Sweden: 27%, Belgium: 28%, Poland: 29%, Germany: 29%. 'European Advertising Consumer Research Report 2021' (*European Interactive Digital Advertising Alliance*, 2021), p. 8 <<https://edaa.eu/wp-content/uploads/European-Advertising-Consumer-Research-Report-2021.pdf>>.

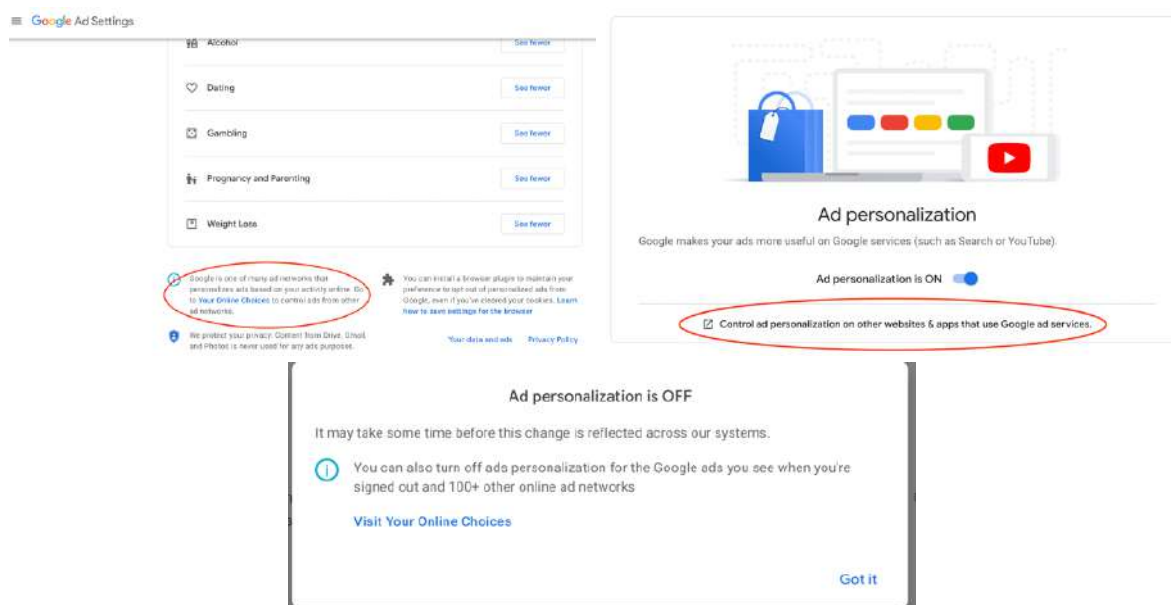


Figure 21: Mention of YOC in Google Ad Settings (May 2022)⁸⁶⁴.

When seeing an ad served by Google on publisher websites and apps, individuals must click on the YourAdChoices Icon⁸⁶⁵, which is different to the icons used by Google and Facebook in their Ad Settings and Ad Preferences tools (see sections 6.4.1.1 and 6.5.1.1). In some cases, individuals are directed through a series of pop-up windows displayed by Google in order to then click on “Why this ad?”, which opens a Google page “About this Ad”, allowing individuals to change their Google Settings. In some cases, the “About this Ad” page opens directly. The individual must scroll down to the bottom of the page to find the link to access the tool (see figure 22). The way it is designed suggests the information is ancillary to the settings and less relevant for users.

⁸⁶⁴ ‘Ad Settings - Ad Personalization’ (Google Ad Settings) <<https://adssettings.google.com/>> accessed 19 May 2022.

⁸⁶⁵ ‘YourAdChoices’ (Digital Advertising Alliance) <<https://youradchoices.com/>> accessed 19 May 2022.

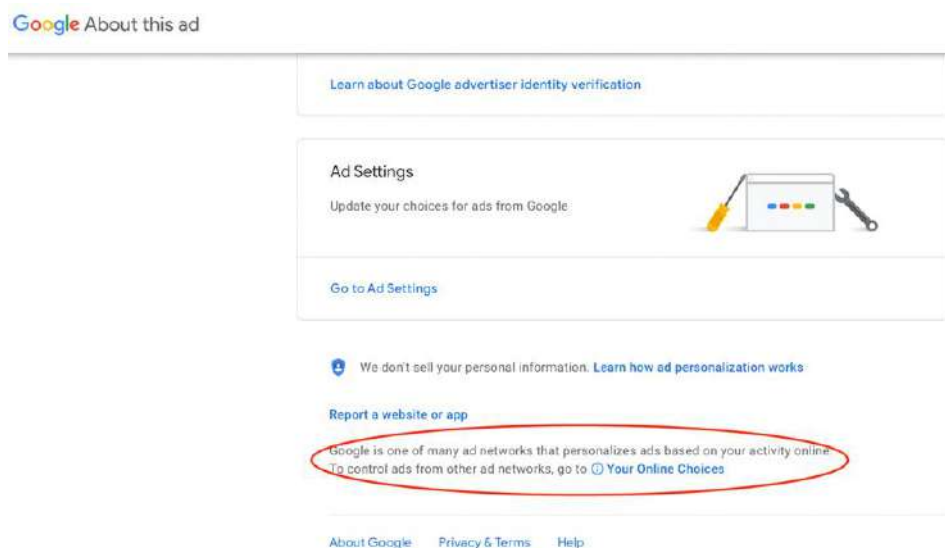


Figure 22: Mention of YOC in the "About this Ad" page (May 2022)⁸⁶⁶.

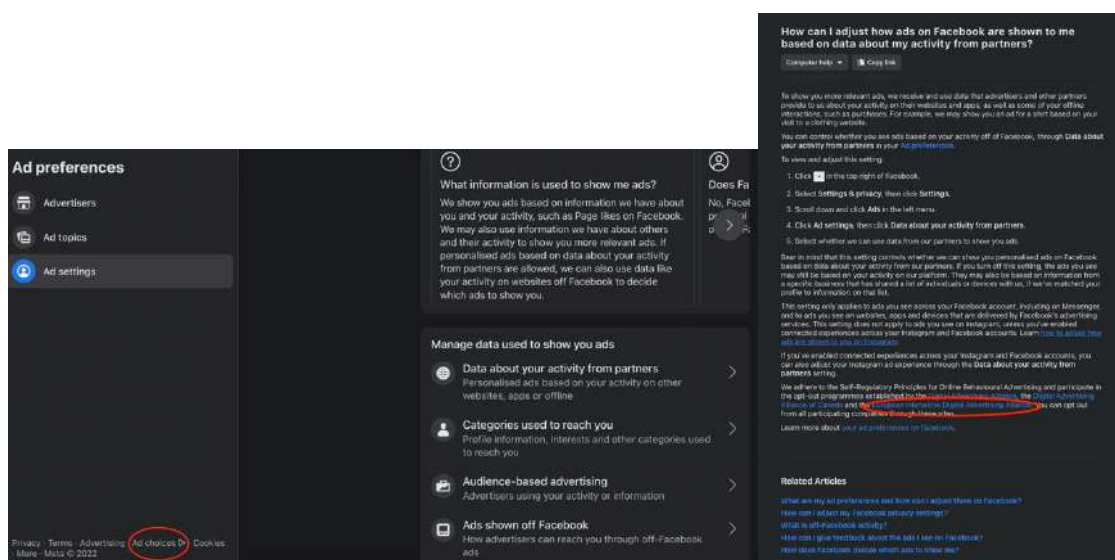


Figure 23: Access to youronlinechoices.eu through Facebook Ad Preferences⁸⁶⁷ and Facebook Help Centre (May 2022)⁸⁶⁸.

YOC can also be accessed through Facebook Ad Preferences but this is difficult to do in practice. Users must first be able to recognise the AdChoices icon at the bottom of the page, which is in a smaller font (see figure 23). In Google Ad Settings the placement and the way it is designed suggests the information is

⁸⁶⁶ 'About this Ad' (Google Ad Settings) <<https://adssettings.google.com/whythisad>>, accessed 3 May 2022.

⁸⁶⁷ 'Facebook Ad Preferences' (Facebook Ad Preferences) <https://www.facebook.com/adpreferences/?entry_product=waist>, accessed 3 May 2022.

⁸⁶⁸ 'How can I adjust how ads on Facebook are shown to me based on data about my activity from partners?' (Facebook Help Centre) <<https://www.facebook.com/help/568137493302217>> accessed 23 May 2022.

ancillary to the settings and less relevant for users. Moreover, the link does not lead users to the youronlinechoices.eu page but to a Facebook Help page which explains how to change ad settings on Facebook. When scrolling down to the bottom of the page, the link to youronlinechoices.eu can be found if users click on “European Interactive Digital Advertising Alliance”, which is different from the AdChoices icon users clicked on previously. For most users, the two names are not related and, contrary to the Google settings described above, the information on the Help Centre does not explain the purpose of the YOC tool to users.

6.6.2 Comprehension

The YOC interface, titled “Your Ad Choices” is a list of companies which collect personal data through the websites that users visit. The explainer paragraph is short but uses technical language (see figure 24).

Within the list, each company provides its own information, which is most of the time a description of the company with no information regarding data collection or targeting. The language used is unclear, the list of companies is long (at the time of this review, the list included 84 companies) and the average user is unlikely to be familiar with the majority of the companies listed.

There are other sections on the website which are intended to provide information on advertising and on the tool. The language used is technical and the amount of information is, in some cases, overwhelmingly detailed.

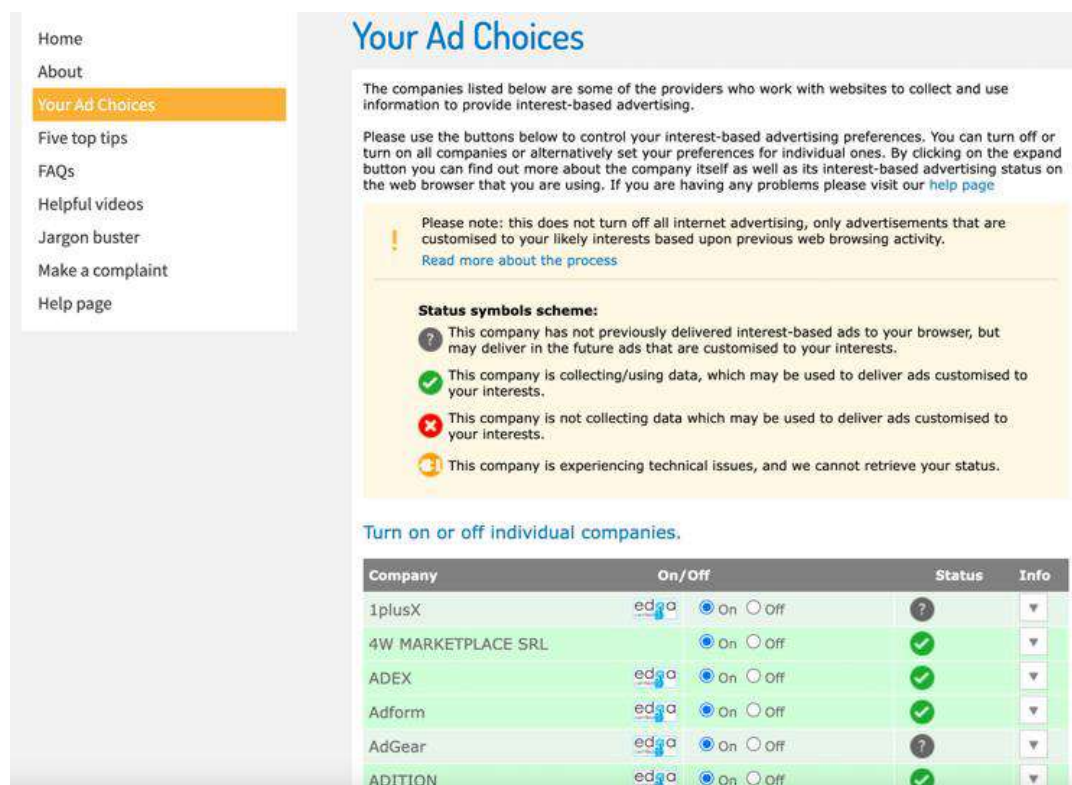


Figure 24: The YOC interface (May 2022)⁸⁶⁹.

6.6.3 Action

The website is not user-friendly in terms of design and suffers from major usability flaws. First, the option to turn on or off all the companies at once only appears via a pop-up if the individual scrolls the list up or down. Depending on the browser used, their choices are sometimes not reflected at all (nothing happens), or some companies are still not included and cannot be turned on or off. Additionally, the pop-up does not reappear immediately once a choice has been made, so if an individual changes their mind, they must wait a couple of minutes or reload the website and wait for the pop-up to re-appear. The mobile version has the same issues.

It should be noted that the page indicates that deleting browser cookies can remove the preferences made using this site and that individuals must therefore visit the page periodically to review their preferences, which is inconvenient.

⁸⁶⁹ 'Your Ad Choices' (*Your Online Choices*) <<https://www.youronlinechoices.com/ie/your-ad-choices>> accessed 3 May 2022.

6.6.4 Conclusion

The tool is not user-friendly. It is difficult to access, and the intersection between this tool and others (e.g. Google Ad Settings and Facebook Ad Preferences) is not clear. It is hard for individuals to understand how the changes made using this tool apply to the ads they see in different places online. Moreover, the design, usability flaws and the language of the website make it a difficult tool to use.

6.7 Apple's App Tracking Transparency Framework

In 2021, Apple updated the way that individuals are offered choices regarding data collection by third parties on devices running the Apple operating system iOS, known as App Tracking Transparency (ATT). ATT prompts are displayed to the majority of users who interact with apps that use tracking. Prompts are not shown to users with older iOS versions (pre-dating iOS 14.5) or users who have opted to automatically deny all requests via the device's settings. Prompts are also not shown to users who have tracking restricted by default (approximately 5% of users), typically because their Apple ID shows them as being under the age of 18.

Research from mobile analytics provider Flurry estimates that as of April 2022, only 25% of users worldwide opt in to tracking, suggesting that the ATT prompts have empowered a significant share of Apple users to indicate their data collection preferences⁸⁷⁰. This is consistent with estimates collated by the UK Competition and Markets Authority (CMA), which generally place opt-in rates at 20-30%⁸⁷¹. However, some figures suggest that users opting in to tracking may be doing so without full awareness of what they are consenting to. One survey found that when asked why they "clicked allow" on the prompts, 25% of users responded that they were not sure, "so it felt safer to just select allow"⁸⁷². Indeed, the CMA suggests that Apple did not conduct any user testing of the design of the ATT prompt and argues that the use of the word "choice" "may not maximise user comprehension and thus may not help consumers to make effective choices"⁸⁷³. More specifically, the CMA argues that the use of the word "track" in particular

⁸⁷⁰ 'App Tracking Transparency Opt-In Rate - Monthly Updates' (*Flurry*, 2 May 2022)

<<https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/>> accessed 19 May 2022.

⁸⁷¹ 'Appendix I: Considering the Design and Impacts on Competition of Apple's ATT Changes' in 'Online Platforms and Digital Advertising - Market Study Final' (*CMA*, 2020)

<https://assets.publishing.service.gov.uk/media/61b86aee8fa8f5037ffaa347/Appendix_I_-_Considering_the_impacts_of_Apples_ATT.pdf>.

⁸⁷² Hill A, 'What Consumers Really Think of the IDFA Prompt' (*On Device Research*, May 2021)

<<https://ondeviceresearch.com/blog/what-consumers-really-think-of-the-idfa-prompt>> accessed 19 May 2022.

⁸⁷³ 'Appendix J: Apple's and Google's Privacy Changes' in 'Mobile Ecosystems Market Study Final Report' (*CMA*, 2022)

<https://assets.publishing.service.gov.uk/media/62a229c2d3bf7f036750b0d7/Appendix_J_-_Apple_s_and_Google_s_privacy_changes_eg_ATT_ITP_etc_-_FINAL.pdf>.

“can lead to users misunderstanding the scope of the ATT framework”. They furthermore note that “such choice architecture could unduly influence some consumers to refuse data sharing in a way that may be inconsistent with their preferences”.

6.7.1 Access

The prompt automatically appears when an app wants to track individuals or access their device’s advertising identifier. It is a user-friendly way for individuals to state their preferences, as they do not have to look for it in the settings and they do not need to take any proactive steps to access their preferences.

Although the prompt does not mention this possibility, users can also go to their device’s settings and turn off tracking in order to “automatically deny” all new requests. This can be accessed through four steps (click on “Settings” -> then “Privacy” -> then “Tracking” -> then turn off the button “Allow Apps to Request to Track”, see figure 25).

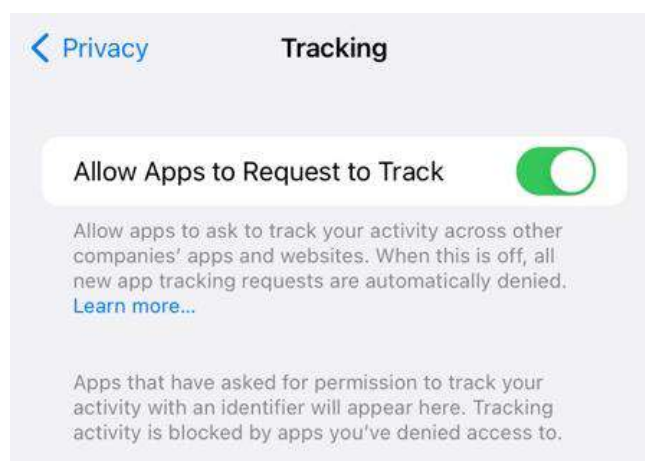


Figure 25: Apple's tracking settings (May 2022).

6.7.2 Comprehension

Apple’s settings use simple and short sentences, which are easy for users to understand. However, this limited information can also be a barrier to making an informed choice.

The prompt contains a mandatory question (“Allow X to track your activity across other companies’ apps and websites?”) and two options (“Ask App Not to Track” or “Allow”, see figure 26). The simple and clear language is easy to understand. Apps can also include a purpose in the prompt that explains why they would like to track the individual. The language differs depending on the app, but most apps

reviewed used the same or a similar standardised sentence, which is short and easy to understand (see figure 26, on the left). Other apps might use longer sentences or paragraphs which are less user-friendly and less easy to understand (see figure 26, on the right).

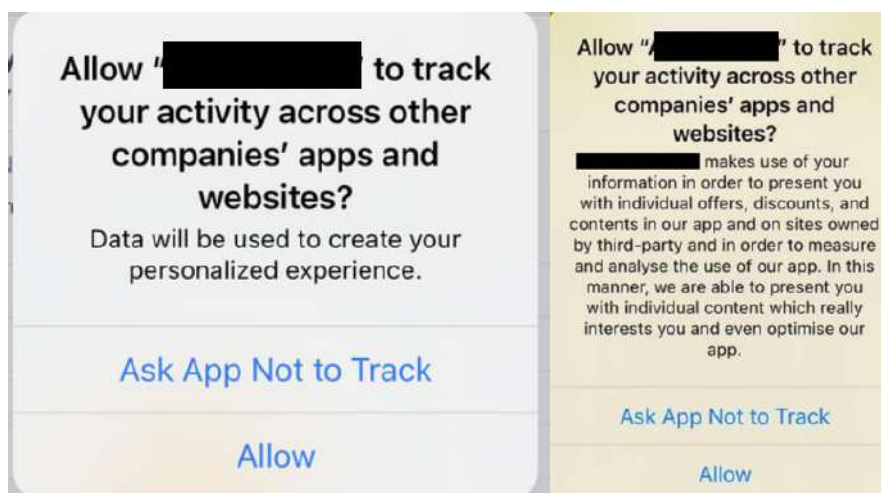


Figure 26: Examples of Apple's app tracking consent prompts (May 2022).

6.7.3 Action

Individuals can easily state their preferences using the settings and the prompt. One click is sufficient to either turn on or off the tracking requests in the settings or to indicate the choice in the prompt. Moreover, the choice is definitive meaning individuals do not have to state their preferences every time they use an app (though it can still be changed in settings).

6.7.4 Conclusion

The consent prompts that Apple's ATT provides are user-friendly, easily accessible, comprehensible and actionable. The prompt is automatically provided to users, meaning they do not need prior knowledge of it to be able to use it. Additionally, it is quick to use, with straightforward explanations. However, the option to automatically reject tracking requests is more difficult to access, as it is not presented along with the prompts.

6.8 Key findings

This review points to significant deficiencies in most of the tools which were reviewed in April and May 2022 to indicate individual preferences for data collection and targeting for digital advertising. User-friendly access is a notable

issue, as is comprehensibility of information and ease of use. On balance, the tools assessed lack user-friendliness to varying extents and feature a multitude of design features and language choices that undermine the ability of users to exercise control over their own data.

These deficiencies are compounded by the fact that individuals are required to indicate their preferences across all of these tools separately in order to influence the way that ads are targeted to them across all the devices, apps and sites they use. This is difficult to understand and, most likely, extremely confusing for individuals, especially children. This lack of consistency and interoperability prevents individuals from exerting meaningful control over how their data is used for digital advertising purposes. The DSA will introduce provisions for individuals to have access to more transparency over how ads are targeted to them: Articles 26 and 39 DSA provide for enhanced transparency on targeting parameters and for individuals to be informed about how to change parameters “where applicable”. However, this is unlikely to address some of the issues that have surfaced in this review related to indicating and applying targeting preferences, especially the challenge of trying to do this across the complex and opaque ecosystem of companies that process individuals’ personal data for advertising purposes.

7 How does the existing regulatory framework address the issues raised in this study?

This study has shown that advertisers and publishers currently encounter a range of issues related to digital advertising which contribute to reducing incentives to test and adopt alternative advertising models. This section will explore the extent to which some of these issues are addressed within the current regulatory framework, including proposed instruments.

7.1 The General Data Protection Regulation

The General Data Protection Regulation (GDPR) provides data subjects with the right to object to the processing of personal data for direct marketing at any time, including profiling (Article 21.2 GDPR). This applies to both “initial or further” processing (Recital 70 GDPR). The proposed ePrivacy Regulation would introduce a harmonised definition of “direct marketing” in EU law. Although the final text has not yet been agreed in trilogue, the definitions proposed by the European Commission, the European Parliament and the Council all include references to digital advertising “to one or more identified or identifiable” end-users. Since all types of advertising referenced in section 1 use individuals’ personal data in some form to target ads to them, this definition – and therefore the “right to object” of Article 21.2 GDPR – could apply. In the absence of an agreement on the ePrivacy Regulation, several national data protection authorities (DPAs) have published definitions of direct marketing which, again, could all be understood to extend to the types of digital advertising referenced in section 1.

The GDPR states that the right to object to data processing for direct marketing must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information” (Article 21.4 GDPR). Article 21.5 GDPR provides for this right to be exercised “by automated means using technical specifications”. Although some of the ad preference tools reviewed in section 6 do offer users the ability to “turn off” ads that are targeted to them based on their personal data, our evaluation concluded that the majority of these tools are not easy to access and therefore not “explicitly brought to the attention of the data subject”. In addition, it is not clear to what extent these tools could be considered as an exercise of the rights provided for in Article 21.2 GDPR because there is not sufficient transparency around the actions companies take in response to the use of these tools with regards to data processing.

Further, the right to object in Article 21.2 GDPR has not been subject to regulatory or court action, resulting in questions as to its scope and reach. For instance, it is

unclear if the right to object under Article 21.2 GDPR provides a basis for individuals to object to being subject to profiling or allocated interest categories by social media companies entirely, where those social media companies rely on personalised advertising for their business model.

In addition, research has suggested that multiple, possibly hundreds, of separate entities can access advertising data every time a webpage is accessed⁸⁷⁴. The absence of any centralised mechanism to register objections to processing results in individuals needing to expend significant effort when looking to indicate their data collection preferences in this way. This issue is aggravated by the lack of transparency of all the companies that collect data about them for digital advertising purposes. This information is usually provided in various different documents spread across the different sites and apps that the person uses (e.g. privacy policies, cookie policies and information notices, account settings). It would be extremely difficult for a child to navigate this maze of information.

Several data protection authorities have issued decisions which rule that some data processing practices that are widespread in the digital advertising industry are not compliant with GDPR.

- In 2022, the Belgian data protection authority, the Autorité de protection des données (APD), found that the Transparency and Consent Framework (TCF), developed by IAB Europe, fails to comply with a number of provisions of the GDPR. The TCF underpins the way that data is shared and processed in real-time bidding (RTB), a standard used for programmatic display advertising⁸⁷⁵. This decision is linked to a complaint filed by several individuals and NGOs in 2019⁸⁷⁶. IAB Europe has submitted an action plan to the APD which “should enable a version of the TCF with a broader complaint functionality to be rolled out over a 6-month period under the supervision of the APD”. Meanwhile, IAB Europe has also filed an appeal against the APD’s decision which has led to the case being referred to the European Court of Justice (CJEU)⁸⁷⁷.

⁸⁷⁴ ‘The Biggest Data Breach - ICCL Report on the Scale of Real-Time Bidding Data Broadcasts in the U.S and Europe’ (*Irish Council for Civil Liberties*, 16 May 2022) <<https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>>.

⁸⁷⁵ ‘Decision on the Merits 21/2022 of 2 February 2022 Concerning: Complaint relating to Transparency & Consent Framework’ (*Autorité de protection des données*, 2022), <<https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>>.

⁸⁷⁶ Johnny Ryan, Pierre Dewitte, Jef Ausloos, Katarzyna Szymielewicz (with the NGO Panoptykon Foundation acting on her behalf), and the NGOs Bits of Freedom and La Ligue des Droits de l’Homme.

⁸⁷⁷ ‘Case of IAB Europe against the Data Protection Authority 2022/AR/292’ (7 September 2022) <<https://www.gegevensbeschermingsautoriteit.be/publications/tussenarrest-van-7-september-2022-van-het-marktenhof-ar-292.pdf>>.

- In 2021, the Norwegian data protection authority (Datatilsynet) found that Grindr was unlawfully sharing personal data with third parties for digital advertising purposes⁸⁷⁸, linked to a GDPR complaint filed by the Norwegian consumer council, Forbrukerrådet, in 2020. It has been reported that Grindr is appealing this decision on the grounds that it “appears to want to hold Grindr – a relatively small player in a much larger ecosystem – responsible for industry-wide practices”⁸⁷⁹. The company also claims that the decision reflects “incorrect interpretations of the GDPR”⁸⁸⁰.
- In 2019, the French data protection authority, Commission Nationale Informatique et Libertés (CNIL), imposed a fine on Google for “lack of transparency, inadequate information and lack of valid consent”⁸⁸¹ related to digital advertising, linked to a GDPR complaint filed by noyb and La Quadrature du Net in 2018. Although this decision was appealed by Google, the French Conseil d’Etat confirmed the ruling in June 2020. The Conseil d’Etat also did not allow Google to appeal the decision to the Court of Justice of the European Union (CJEU).⁸⁸²
- Additionally, several other complaints filed against Meta (covering Facebook, Instagram and WhatsApp) and Google are still being investigated by the Irish Data Protection Commission (DPC)⁸⁸³. This includes a complaint filed in 2020 relating to alleged infringement of rules on purpose limitation due to the way personal data is combined across different sites, apps and services owned by a digital advertising gatekeeper (Google)⁸⁸⁴.

⁸⁷⁸ ‘Administrative Fine - Grindr LLC’ (*Datatilsynet*, 2021), <<https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/>>.

⁸⁷⁹ Fried I, ‘Exclusive: Grindr to Appeal Norwegian Fine for Privacy Violations’ (*Axios*, 14 February 2022) <<https://www.axios.com/2022/02/14/grindr-appeal-norwegian-fine-privacy>> accessed 8 September 2022

⁸⁸⁰ Fried I, ‘Exclusive: Grindr to Appeal Norwegian Fine for Privacy Violations’ (*Axios*, 14 February 2022) <<https://www.axios.com/2022/02/14/grindr-appeal-norwegian-fine-privacy>> accessed 8 September 2022

⁸⁸¹ ‘The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC’ (*European Data Protection Board*, 21 January 2019) <https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en> accessed 8 September 2022.

⁸⁸² ‘Base de Jurisprudence - Decision N° 430810’ (*Conseil d’État*, June 2020) <<https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/430810>>.

⁸⁸³ ‘Annual Report 2021’ (*Data Protection Commission*) <https://dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf> p. 57-64.

⁸⁸⁴ Ryan J, ‘Formal GDPR Complaint against Google’s Internal Data Free-for-all’ (*Brave*, 16 March 2020), <<https://brave.com/google-internal-data-free-for-all/>>.

However, to date, there is little evidence that the regulatory action outlined above has led to significant changes to the structure and functioning of the digital advertising ecosystem as it pertains to personal data. The GDPR may be a contributing factor to the industry's shift away from third-party data (see section 1) but our research indicates that the volume and nature of personal data processing in digital advertising has not significantly changed since the complaints related to these cases were filed between 2016-2020.

7.2 ePrivacy

The ePrivacy Directive has been used to challenge the validity of consent for digital advertising purposes in a number of cases, particularly in relation to "cookie banners". In 2020, the French data protection authority CNIL fined Google €150 million for making it harder to refuse than accept cookies that were used to collect data for a number of purposes including digital advertising⁸⁸⁵. The CNIL also fined Amazon €35 million for placing advertising cookies on the computers of users without prior consent or satisfactory information⁸⁸⁶. NGO noyb has launched more than 700 complaints related to cookie banners being used to collect data for advertising purposes, linked to enforcement of the ePrivacy Directive⁸⁸⁷.

The ePrivacy Directive has also been used to challenge large platforms' approaches to applying a legal basis to their data collection practices with regard to digital advertising. For example, in 2022 the Italian data protection authority issued TikTok with a warning that a proposed change to TikTok's privacy policy regarding the legal basis for digital advertising⁸⁸⁸ would infringe the ePrivacy Directive, highlighting the Directive's important role in regulating the collection of

⁸⁸⁵ 'Délibération de La Formation Restreinte N°SAN-2021-023 Du 31 Décembre 2021 Concernant Les Sociétés Google LLC et Google Ireland Limited' (*Commission Nationale de l'Informatique et des Libertés*, December 2021) <<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062>> accessed 9 September 2022.

⁸⁸⁶ 'Cookies: The Council of State Confirms the 2020 Sanction Imposed by the CNIL against Amazon' (*CNIL*, 28 June 2022) <<https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon>> accessed 9 September 2022.

⁸⁸⁷ 'Cookie Banners' (*noyb.eu*) <<https://noyb.eu/en/project/cookie-banners>> accessed 9 September 2022.

⁸⁸⁸ To use legitimate interest as a legal basis instead of consent.

data using cookies and similar tracking technologies⁸⁸⁹. This led TikTok to suspend the planned change⁸⁹⁰.

The European Commission's proposal for an ePrivacy Regulation⁸⁹¹ includes a provision for consent to be expressed using the technical settings of a software application that enables access to the internet (e.g. a browser). This would apply to the consent required for companies to use the processing and storage capabilities of terminal equipment and the collection of information from terminal equipment (e.g. via cookies that collect data for digital advertising purposes, as outlined in section 1.3.1.1). This could complement the right to object to processing outlined above, but it would likely not apply to all cases of data collection linked to digital advertising, such as data collected without the use of cookies or trackers – for example in the context of a first-party relationship between an individual and a company when signing up for an account or subscription. It is also important to note that the industry is increasingly moving away from technologies that involve placing trackers such as cookies on terminal equipment in favour of other forms of identification such as user accounts and email addresses (see section 1.3.1.1.4).

7.3 EU competition law

Articles 101 and 102 Treaty of the Functioning of the European Union (TFEU) have been applied at both EU and Member State level to tackle alleged anti-competitive practices in digital advertising.

- The European Commission issued a fine to Google for using restrictive clauses in contracts with third-party websites to prevent rivals from placing search ads on those websites⁸⁹².

⁸⁸⁹ 'Provvedimento del 7 luglio 2022 [9788429]' (*Garante per la Protezione dei Dati Personali*, 7 July 2022) <<https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9788429>> accessed 9 September 2022; 'TikTok: Italian SA Warns against "personalised" Ads Based on Legitimate Interest' (*European Data Protection Board*, 15 July 2022) <https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads-based-legitimate-interest_en> accessed 9 September 2022.

⁸⁹⁰ 'Tik Tok rinvia la pubblicità basata sul legittimo interesse. Per il Garante privacy "una decisione responsabile"' (*Garante per la Protezione dei Dati Personali*, 12 July 2022) <<https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9789143>> accessed 9 September 2022.

⁸⁹¹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003 (COD) <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications>>.

⁸⁹² 'Commission Decision of 20.3.2019 Relating to a Proceeding under Article 102 of the Treaty on the Functioning of the European Union (the Treaty) and Article 54 of the EEA Agreement (AT. 40411 - Google

- The European Commission is currently investigating whether Meta uses advertising data provided by its advertiser clients to compete with them⁸⁹³.
- The European Commission has launched an investigation into whether Google favours its own services at the expense of rival intermediaries⁸⁹⁴. This investigation will also examine Google's plans to prohibit the placement of third-party cookies on Chrome and replace them with the Privacy Sandbox set of tools.
- The Portuguese competition authority, Autoridade da Concorrência (AdC), opened administrative proceedings against Google for abuse of dominance, based on evidence of "self-preferencing behaviours by Google at various stages of the digital advertising value chain". The European Commission has now extended the scope of its own investigation (see above) to include the practices and markets investigated by AdC⁸⁹⁵.
- The French competition authority ADLC issued a fine and imposed binding commitments on Google for self-preferencing its digital advertising services at the expense of rival intermediaries⁸⁹⁶.
- The German competition authority, the Bundeskartellamt (BKA), issued a decision prohibiting Meta from combining personal data across its different services and from making the use of its services conditional on the collection of personal data. The BKA argues that this behaviour constitutes an abuse of dominant position, which Meta is able to leverage in the social media advertising market in violation of the German Competition Act⁸⁹⁷. The decision is currently being appealed by Meta.

Search (AdSense))' (*European Commission*)

<https://ec.europa.eu/competition/antitrust/cases/dec_docs/40411/40411_1619_11.pdf>.

⁸⁹³ 'Antitrust: Commission opens investigation into possible anticompetitive conduct of Facebook' (*European Commission*, 4 June 2021),

<https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2848>.

⁸⁹⁴ 'Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector' (*European Commission*, 22 June 2021),

<https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143>.

⁸⁹⁵ 'Portuguese Competition Authority's Google Investigation Moves to the European Commission' (*Autoridade da Concorrência*, 9 September 2022)

<<https://www.concorrencia.pt/en/articles/portuguese-competition-authoritys-google-investigation-moves-european-commission>> accessed 7 October 2022.

⁸⁹⁶ 'Decision 21-D-11 of June 07, 2021 Regarding Practices Implemented in the Online Advertising Sector' (*Autorité de la Concurrence*, 2021), <<https://www.autoritedelaconcurrence.fr/en/decision/regarding-practices-implemented-online-advertising-sector>>.

⁸⁹⁷ 'Case B6-22/16 Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing' (*Bundeskartellamt*, 2021),

Some competition authorities have raised concerns about some of the models being proposed as part of the industry's shift away from third-party data, particularly Google's Privacy Sandbox proposals (see section 5). So far, this has led to Google making specific commitments to ensure compliance with competition law (for example, commitments made to the UK Competition and Markets Authority (CMA))⁸⁹⁸. However, as the Privacy Sandbox proposals are still in development it is not yet possible to assess the real impact of regulatory action in this context. Nevertheless, this has demonstrated that the EU regulatory framework for competition law can enable a proactive approach to engaging in the development of new digital advertising technologies.

Some of the national competition authorities interviewed for this study expressed a view that although there have been several competition decisions related to digital advertising, speed and resources can be a barrier to effective regulation in this context. Several stakeholders also pointed to the need for dialogue between competition and privacy authorities. Interviewees at one national competition authority suggested that large platforms have significantly higher budgets than competition authorities and questioned whether fines imposed on them are dissuasive enough. Multiple interviewees from national competition authorities pointed to the Digital Markets Act (DMA) as a potential positive step forward in this regard, with one interviewee describing it as "designed to solve the problem of limitations of lengthy interventions in competition enforcement once the contravention has already taken place".

7.4 Environmental initiatives

The environmental impact of waste in the digital advertising supply chain is generally overlooked in existing legislation and is seldom mentioned in the set of initiatives proposed under the European Green Deal. Although there are no measures specifically targeting waste from digital advertising, some of the broader initiatives linked to the European Green Deal could be relevant to addressing this issue. For instance, the proposed recast Energy Efficiency Directive identifies emissions from information and communication technologies (ICTs) as a cause for concern, in particular emissions from data centres⁸⁹⁹. Accordingly, it sets out

<<https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html>>.

⁸⁹⁸ 'CMA Secures Improved Commitments on Google's Privacy Sandbox' (*Competition and Markets Authority*, 26 November 2021) <<https://www.gov.uk/government/news/cma-secures-improved-commitments-on-google-s-privacy-sandbox>> accessed 9 September 2022.

⁸⁹⁹ See Recital 66 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

measures requiring the public disclosure of data centres' energy consumption by 2024, as well as suggesting a possible Union-wide sustainability rating scheme for data centres⁹⁰⁰. Greater transparency as to the energy consumption of data centres could potentially help measure digital ad-related energy consumption. Large platforms may fall within the Article 11 Energy Efficiency Directive requirement that enterprises above a certain level of annual energy consumption implement an "energy management system" composed of elements such as the "monitoring of actual energy consumption, actions taken to increase energy efficiency, and measurement of progress"⁹⁰¹. Though potentially beneficial to efficiency and transparency more generally, these measures may not directly impact the broader structural causes of emissions linked to digital advertising identified in section 2 or significantly incentivise advertisers and investors to switch to more sustainable alternative digital advertising models. Overall, the issue of digital advertising emissions is not expressly addressed in legislation, whether through the European Green Deal or other initiatives.

7.5 Digital Markets Act

The Digital Markets Act (DMA) points out that the conditions under which gatekeepers provide digital advertising services to businesses, including both advertisers and publishers, "are often non-transparent and opaque"⁹⁰² and that this "undermines their ability to switch between undertakings providing online advertising services"⁹⁰³. Article 6.8 DMA is designed to "further enhance fairness, transparency and contestability of online advertising services"⁹⁰⁴ by requiring gatekeepers to provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, with "access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements

⁹⁰⁰ Article 11 and Article 31 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

⁹⁰¹ Article 11 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

⁹⁰² Recital 45 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁹⁰³ Recital 45 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁹⁰⁴ Recital 58 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

inventory, including aggregated and non-aggregated data⁹⁰⁵. Articles 5.9 and 5.10 DMA also require gatekeepers to provide information about pricing and fees to publishers and advertisers.

These measures could go some way to improving the availability of data for advertisers and publishers to make evidence-based decisions, but some industry experts consulted for this study (including advertisers and publishers) have pointed to possible limitations of these provisions that would need to be addressed in order to meaningfully improve transparency in the digital advertising ecosystem.

Firstly, they argue that the DMA's reference to "aggregated and non-aggregated" data is too broad. One representative of an advertiser association who has been involved in initiatives designed to improve transparency in the digital advertising industry suggested that advertisers need access to detailed "log-level" data in order to achieve effective transparency and enable the level of analysis needed to make evidence-based decisions about media investment.

Secondly, they point out that it would also be important for all the data referenced in Articles 5.9, 5.10 and 6.8 DMA to be provided in a standardised format so that comparisons can be made across different platforms.

There are also concerns that the DMA's main limitation regarding advertising transparency is its scope. Large platforms and publishers interviewed for this study pointed out that transparency requirements in the digital advertising industry need to apply to all actors in the supply chain, not just gatekeepers that fall within the scope of the DMA.

Articles 5.2(b), (c) and (d) DMA would prohibit companies designated as gatekeepers from combining and/or cross-using personal data across different services they provide. This could restrict large platforms' ability to gain a competitive advantage by leveraging the large amounts of data generated by individuals across the different services they provide, thereby potentially enabling publishers that collect first-party data from their readers to compete more effectively with large platforms. As outlined in section 4, many advertisers and publishers currently feel that this is not possible given the amount of first-party data that large platforms potentially have access to.

Article 5.2(a) DMA would prohibit gatekeepers from processing the "personal data of end users using services of third parties that make use of core platform services

⁹⁰⁵ Article 6.8 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

of the gatekeeper” for the purpose of providing digital advertising services. This could be seen as a way to prevent large platforms that provide publishers with intermediary services from leveraging the data generated on publisher sites to target ads to individuals in other contexts (see section 4).

However, it is important to note that gatekeepers would still be able to combine and/or cross-use data across services if the user has “been presented with the specific choice and has given consent”. Some advertisers and publishers consulted for this study argue that gatekeepers are well positioned to fulfil this requirement given that they tend to have strong first-party relationships with their users. Furthermore, the DMA specifies that gatekeepers should inform users that “not giving consent can lead to a less personalised offer”⁹⁰⁶, which may lead to individuals having an incentive to provide consent in order to benefit from non-ad related personalisation benefits (e.g. remembering history, saving passwords).

Some commentators also predict that there will be debate over what constitutes “specific choice” in this context, as well as the GDPR’s requirements for consent to be “freely-given, specific, informed and unambiguous”. Some critics have pointed to examples of cookie banner designs which do not fulfil these requirements yet have been widely used for several years without enforcement action being taken⁹⁰⁷.

In an interview for this study, Meta flagged that these provisions would not apply to companies which are not designated as gatekeepers and argued that there was a need to ensure that rules are applied uniformly to all companies in the ad tech sector, otherwise there would be gaps in the regulatory framework.

7.6 Digital Services Act

Articles 26 and 39 Digital Services Act (DSA) provide for enhanced transparency on targeting parameters but do not impose any obligations to enable individuals to control or change these parameters if they want to. Article 26 DSA provides that individuals should be informed about how to change parameters “where applicable”. The DSA provides for voluntary codes of conduct on digital

⁹⁰⁶ Recital 37 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

⁹⁰⁷ See, for example, Nouwens M and others, ‘Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence’, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020) <<http://arxiv.org/abs/2001.02479>> accessed 9 September 2022.

advertising⁹⁰⁸ covering an open-ended list of issues, including, but potentially not limited to, the transmission of information held by providers of intermediaries to recipients of the service required by Article 26 DSA, the transmission of information held by providers of intermediaries to the ad repositories provided by very large online platforms and very large search engines, as well as the provision of meaningful information on data monetisation. Such measures might also be supported by further standardisation activities covered by the DSA.

Article 25 DSA introduces provisions that prohibit providers of online platforms to “design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions”⁹⁰⁹. If this provision were applied to some of the ad settings tools reviewed in section 6, it is possible that it could lead to improvements in user-friendliness. However, given that many of these tools provide individuals with choices about how their personal data is processed for digital advertising, it would be possible to argue that they would not fall within the scope of Article 25 DSA because practices covered by GDPR and the ePrivacy Directive are specifically excluded⁹¹⁰.

It is also important to note that Articles 25, 26 and 39 DSA only apply to providers of online platforms⁹¹¹ (Articles 25 and 26 DSA) and very large online platforms⁹¹²

⁹⁰⁸ Article 46 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹⁰⁹ Article 25 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹⁰ Article 25.2 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹¹ According to Article 3(i) DSA, “online platform” means “means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.” 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹² According to Article 33.1 DSA, very large online platforms and very large online search engines are “online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to [Article 33.4].” Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services

and very large online search engines (Article 39 DSA). This means that these provisions would not necessarily apply to all advertising displayed to individuals, for example ads displayed on a small news website.

The DSA introduces a number of provisions related to the way that personal data is used in a digital advertising context. Articles 26 and 28 DSA aim to protect minors⁹¹³ and mitigate negative effects linked to targeting techniques that could “negatively impact entire groups and amplify societal harms”⁹¹⁴. Article 26 DSA introduces a prohibition on providers of online platforms to present advertising “based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679”⁹¹⁵. Article 28 DSA introduces a prohibition on providers of online platforms to present advertising on their interfaces based on profiling “when they are aware with reasonable certainty that the recipient of the service is a minor”⁹¹⁶.

Google and Facebook, the two biggest online platforms in terms of advertising revenue in the EU (see section 1), already claim to restrict the use of “sensitive interest categories” in “personalised ads”⁹¹⁷ (Google) and “detailed targeting options that relate to topics people may perceive as sensitive” (Meta)⁹¹⁸. Many of Google and Facebook’s restrictions align broadly with the GDPR’s definition of special category data, with some exceptions and additions in both cases – see table 12 for more detail.

and amending Directive 2000/31/EC (Digital Services Act), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹³ Recital 71 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹⁴ Recital 69 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹⁵ Article 26.3 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹⁶ Article 28 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹¹⁷ ‘Personalized Advertising’ (*Google Ads Policy Help*) <<https://support.google.com/adspolicy/answer/143465?hl=en>> accessed 9 September 2022.

⁹¹⁸ ‘Updates to Detailed Targeting’ (*Meta Business Help Centre*) <<https://www.facebook.com/business/help/458835214668072>>.

Google's advertising policies disable "ad personalisation" on Google Accounts of "people above the digital age of consent but under 18"⁹¹⁹. Meta restricts a number of targeting options to people under the age of 18, including targeting based on interests, behaviours and demographics⁹²⁰.

This suggests that the prohibitions introduced in Article 26.3 and 28 DSA echo measures which Google and Meta have already put in place, although it is important to note that Meta only removed some of these targeting options in March 2022 while the DSA was going through trilogue negotiations.

Some stakeholders, including advertisers and civil society, have questioned whether the DSA's focus on advertising "based on profiling" could leave room for minors to be targeted if no profiling is used, and give the example of a user that provides their age explicitly when signing up for a service or makes this information available on a profile. Similarly, some civil society stakeholders have expressed concern that the wording of Article 26.3 DSA is not sufficiently precise to prohibit non-special category data from being combined and inferred to create new targeting options which could be considered sensitive, for example targeting individuals based on an interest in certain topics known to be linked – albeit not explicitly – to areas such as sexual orientation, religion or health. They have also pointed out that restricting Article 28 DSA only to cases where the online platform is "aware with reasonable certainty that the recipient of the service is a minor" could limit the impact of this provision. However, it is important to note that the scope of the provisions in the DSA inherits the interpretation of "profiling" as laid out in the GDPR. Official guidance in the context of the GDPR clarifies that profiling includes – but is not limited to – inferences made from different data points. Profiling is defined in the GDPR "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"⁹²¹. In addition, it is noteworthy that the DSA text uses the notion to characterise the type of ads which may not be presented on the online interface of an online platform, rather than prohibiting the processing of personal data or specifying which processor (e.g. the platform, an intermediary, an advertiser) would have been engaging in profiling.

⁹¹⁹ 'Ad-Serving Protections for Teens' (*Google Ads Policy Help*) <https://support.google.com/adspolicy/answer/12205906?hl=en&ref_topic=1626336> accessed 9 September 2022.

⁹²⁰ 'About Advertising to Young People' (*Meta Business Help Centre*) <<https://www.facebook.com/business/help/229435355723442>>.

⁹²¹ Article 4.4 GDPR. *EU General Data Protection Regulation (GDPR)*: 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), OJ 2016 L 119/1.

GDPR category (Article 9)	“special data”	Google “sensitive interest categories”	Meta “topics people may perceive as sensitive”
Processing of personal data revealing: <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership Processing of: <ul style="list-style-type: none"> • Data concerning a natural person’s sex life or sexual orientation • Data concerning health • Genetic data • Biometric data for the purpose of uniquely identifying a natural person 	<ul style="list-style-type: none"> • Race and ethnicity • Political affiliation • Religious belief • Trade union membership • Sexual orientation • Membership in a marginalised or vulnerable social group • Transgender identification • Personal health content • Personal financial distress, difficulties or deprivation • Personal hardships with family, friends or other interpersonal relationships • Personal criminal record, crimes committed, criminal allegations or criminal charges • Personal status as a victim of abuse, crime or other traumatic event 	Targeting options referencing causes, organisations or public figures that relate to: <ul style="list-style-type: none"> • Race and ethnicity • Political affiliation • Religion • Sexual orientation • Health 	

Table 12: Summary of “sensitive” categories that Google and Meta restrict ad targeting against, compared to the GDPR definition of “special category” data (retrieved September 2022).

Conversely, it is also important to note that Articles 26 and 28 DSA would only apply to advertising “presented” on an online platform’s “interface” (Article 28 DSA) or to “recipients of the service” of the online platform (Article 26.3 DSA). This means that advertising based on profiling could still be targeted to minors or based on special category data on sites and apps that are not considered “online

platforms” within the meaning of Article 3(i) DSA⁹²². It is possible that this may include advertising on a number of different sites and apps belonging to news publishers and other types of content, including programmatic ads delivered by intermediaries.

7.7 EU consumer protection law

Although the use of cookies and the provision of valid consent are regulated by the ePrivacy Directive and the GDPR, EU consumer protection laws provide additional grounds for ensuring that business-to-consumer practices are fair and transparent, including when they involve the use of cookies for digital advertising purposes. Even if the service is provided as free of monetary payment, the business model is commercial as it implies subjecting the user to advertising and therefore falls under EU consumer protection law.

In particular, under the Unfair Commercial Practices Directive (UCPD), any manipulative practice that materially distorts or is likely to distort the economic behaviour of an average or vulnerable consumer could breach the trader’s professional diligence requirements or amount to a misleading or aggressive practice, depending on the specifics of the practice under examination. In order to comply with consumer law, traders should therefore take appropriate measures to ensure that the design of their interface does not distort the transactional decisions of consumers and allows them to make free choices.

Manipulative practices to obtain consent are likely to qualify as a misleading action under Article 6 UCPD, or as a misleading omission under Article 7 UCPD by making the information unintelligible or ambiguous. Moreover, using emotion to steer users away from making a certain choice could amount to an aggressive practice under Article 8 UCPD for using “undue influence” to impair the consumer’s decision-making.

Behavioural studies have shown that default settings have a significant impact on the transactional decision of an average consumer. Unfavourable default settings in cookie consent banners may be considered to have a similar undue influence

⁹²² According to Article 3(i) DSA, an “online platform” means “a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.” 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

on consumers, because they lead consumers to agree to cookies they might have refused if they were given the opportunity to make an informed choice.

Guidance on the application and interpretation of UCPD published in 2021 specifies that the principle-based provisions and prohibitions in the UCPD can be used to address unfair data-driven business-to-consumer commercial practices, including personalisation of advertising, in addition to the ePrivacy Directive and GDPR⁹²³. The guidance refers to manipulative practices that may include “visually obscuring important information or ordering it in a way to promote a specific option (e.g. one button very visible, another hidden; one path very long, another shorter), as well as using trick questions and ambiguous language (e.g. double negatives) to confuse the consumer”. These practices are sometimes used in so-called “cookie banners”, where consent is requested to place tracking technologies to collect data for digital advertising purposes. A study produced by the European Innovation Council and SMEs Executive Agency (EISMEA) on behalf of DG JUST found that 97% of websites/apps covered presented “dark patterns”, the most prominent of which was “hidden information/false hierarchy” consisting of prioritising an option for a given choice with the use of a brighter colour or bigger font, for example to incite the user to accept cookies⁹²⁴. The study also found that preselection was often used to preselect options most favourable to the website/app especially in settings, for example for privacy settings, ad personalisation and cookie settings.

⁹²³ Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance), C/2021/9320 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29&qid=1640961745514>>.

⁹²⁴ ‘Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation’ (European Commission, April 2022) <<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>>.

8 Areas for further analysis

This study has presented evidence for a number of issues from the perspective of advertisers and publishers that may prevent the development of a sustainable digital advertising ecosystem. They can be grouped into three categories:

- Firstly, the need for improving transparency and accountability in the digital advertising ecosystem in three particular areas: ad spend and other B2B issues; the collection, use and dissemination of personal data; and environmental impacts.
- Secondly, obstacles that make it harder for advertisers and publishers to “know their audience” and communicate with them directly through advertising.
- And finally, the need to increase individuals’ control over how their personal data is used for digital advertising, including how they avoid unwanted targeting.

It is recommended that these areas be the focus of future reflection and analysis.

8.1 Transparency: summary of the issues

Greater transparency would not only enable advertisers to make evidence-based decisions about where to invest their advertising spend, and enable advertisers and publishers to test alternative models, it would also make the ecosystem more accountable to individuals whose data is processed and to whom ads are targeted, and to supervisory authorities.

Evidence in this study indicates that large platforms, which may in future be designated gatekeepers under the Digital Markets Act (DMA), have enormous power in the digital advertising ecosystem, enabling them to **impose what are often considered unfair terms and conditions on advertisers and publishers**. Advertisers and publishers describe **a sense of “dependency” on large platforms** and often describe the relationship with these players in negative terms. A significant amount of digital advertising revenue flows towards large platforms who compete with publishers to sell ad space next to the content they host, as well as providing intermediary services for publishers and advertisers to buy and sell ads. This dual role creates a “frenemy” dynamic, with some publishers saying that they would lose advertising revenue if they do not work with the large platforms.

Some advertisers and publishers are concerned that **moves by large platforms to restrict third-party tracking on their platforms could create opportunities for gatekeepers to exploit their ownership of essential**

services or access points (such as browsers and operating systems), creating even less transparency and competition in future.

This lack of transparency in the digital advertising ecosystem as a whole seems to lead, according to the evidence assembled in this study, to **major market failures**, which manifests in **15% of advertiser spend – an “unknown delta”, representing around one-third of supply chain costs – that cannot be accounted for**. This furthermore contributes to a lack of accountability for **ad fraud**, which is a major issue in the digital advertising ecosystem today. The extent of ad fraud is unclear, but some estimates indicate that by 2025 more than \$50 billion per year could be reaching organised crime and unfriendly governments as a result⁹²⁵.

8.1.1 Transparency on ad spend, effectiveness, measurement, auditing and fraud

There is a lack of transparency in relation to how advertising spend is distributed across different companies and services when ads are bought and sold in an automated manner (programmatic advertising), as well as data related to effectiveness, measurement, auditing and fraud.

Gatekeepers and data about performance of advertising spend

- To remedy this situation in the context of gatekeepers, **Article 6.8 DMA gives “access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the ad inventory, including aggregated and non-aggregated data”⁹²⁶**. Articles 5.9 and 5.10 DMA also require gatekeepers to provide information about pricing and fees to publishers and advertisers. While this is a good step forward, **smaller advertisers and publishers argue that they do not have the budgetary or personnel resources to do this type of verification, and as a result will continue to rely solely on the analytics provided by large platforms and intermediaries**. Some interviewees told us that even where this data is made available, small- and medium-sized

⁹²⁵ Kotila M, Cuevas Rumin R and Dhar S, ‘Compendium of Ad Fraud Knowledge for Media Investors’ (World Federation of Advertisers & Advertising Fraud Council, 2016) <<https://swa-asa.ch/wAssets/docs/publikationen/de/branchenempfehlungen-swa/WFACompendiumofAdFraudKnowledge.pdf>>.

⁹²⁶ Article 6.8 DMA. 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), OJ 2022 L 265/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>>.

enterprises (SMEs) often do not have the time or the expertise to analyse it in depth.

- To remedy this situation, respondents in this study have suggested that these provisions in the DMA should be complemented with **a mechanism that would also allow independent analysts to access such data, who can publish publicly available analysis of different models, based on data sets that span multiple campaigns and platforms.** (This would have to respect confidentiality of commercially sensitive information as well as applicable data protection rules.) Intermediaries and publishers have informed advertisers that data protection and privacy rules are a barrier to sharing measurement data about the performance of advertising. Some advertisers doubt the legal veracity of this, raising concerns instead that data protection and privacy rules are sometimes used as a way of avoiding accountability, or that they lack guidance on their correct interpretation. More clarity on data protection and data sharing in a digital advertising context, specifically in relation to different players in the supply chain, even in the form of specific and precise rules, could help address this issue. In order to facilitate this data sharing in a lawful and proportionate manner, inspiration could be found in the European Digital Media Observatory's Working Group on platform-to-researcher data access which lays out specific guidance on how platform-to-researcher data access might be achieved in compliance with the GDPR⁹²⁷.
- All the data referenced in Articles 5.9, 5.10 and 6.8 DMA would need to be provided in a standardised format so that comparisons can be made across different platforms. A further clarification of the types of data that need to be shared in the context of Articles 5.9, 5.10 and 6.8 DMA is required. For example, the DMA's reference to "aggregated and non-aggregated" data is not sufficiently precise to mandate the sharing of detailed "log-level" data which advertisers require to make evidence-based decisions about media investment. Advertisers and industry representatives who have direct experience working on industry-led initiatives to improve transparency, such as the cross-industry taskforce set up to respond to UK advertiser association ISBA's programmatic supply chain study in 2020⁹²⁸ and the

⁹²⁷ 'Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access' (*European Digital Media Observatory*, 2022) <<https://edmo.eu/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf>>.

⁹²⁸ 'ISBA/PwC: Update on Stage Two of the Programmatic Supply Chain Transparency Study' (*IAB UK*, 1 June 2022) <<https://www.iabuk.com/news-article/isbapwc-update-stage-two-programmatic-supply-chain-transparency-study>> accessed 9 September 2022.

World Federation of Advertisers' Cross-Media Measurement initiative⁹²⁹, can provide further details regarding the data that needs to be made available in order to enable real evidence-based investment decisions.

Gatekeepers and other intermediaries in the digital advertising supply chain

- By one estimate from 2016, 88% of digital ad clicks are fake⁹³⁰. According to the same study, **ad fraud is likely to represent in excess of \$50 billion by 2025**, even on a conservative basis. To address this apparent market failure, **advertisers require data that can indicate whether interaction with ads is coming from humans compared to bots, as well as better traceability of all traders throughout the digital advertising supply chain**. Without such data, including from actors in the supply chain who are not gatekeepers bound by obligations under the DMA, a significant amount of advertising spend will continue to be wasted because of ad fraud.
- Regulators, government agencies and industry groups have warned of hidden fees or an "ad tech tax" whereby a large and difficult-to-measure portion of advertisers' spend is lost to intermediaries before reaching publishers. A study by PwC for ISBA found **an unattributable 15% of digital advertising spend** which the accounting firm could not attribute or explain. This lack of transparency suggests another market failure that would need to be appropriately addressed.

8.1.2 Transparency on personal data processing

Section 4 demonstrated how, according to advertisers and publishers, the companies they work with to buy and sell advertising do not share enough information about how they collect, share and process personal data of advertising audiences. This has two major implications.

- First, **this prevents an objective understanding of the costs and benefits of using personal data and profiling for advertisers compared to less privacy-intrusive alternatives and/or the benefits of digital advertising in general**. Interviewed advertisers and publishers are increasingly frustrated that some of these practices have an impact on

⁹²⁹ 'Cross-Media Measurement' (*World Federation of Advertisers*)

<<https://wfanet.org/leadership/cross-media-measurement>> accessed 9 September 2022.

⁹³⁰ Kotila M, Cuevas Rumin R and Dhar S, 'Compendium of Ad Fraud Knowledge for Media Investors' (*World Federation of Advertisers & Advertising Fraud Council*, 2016) <<https://swa-asa.ch/wAssets/docs/publikationen/de/branchenempfehlungen-swa/WFACompendiumofAdFraudKnowledge.pdf>>.

their reputation as they do not want to be associated with privacy-invasive or unethical data practices.

- Second, **while advertisers and publishers are concerned about the legality of some of these practices and frustrated about the impact on the reputation of their own brands, they perceive there to be no real alternative to deliver and sell digital advertising.** This means that they will continue to invest in digital advertising tools which have been called into question as long as they are still available on the market, especially since neither the entering into force of the GDPR nor some of the relevant enforcement cases have yet made an impact on this advertising model in practice.
- The GDPR states that the right to object to data processing for direct marketing must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information” (Article 21.4 GDPR). Article 21.5 GDPR provides for this right to be exercised “by automated means using technical specifications”. The proposed ePrivacy Regulation⁹³¹ includes a provision for consent to be expressed using technical settings of a software application enabling access to the internet (e.g. a browser). The GDPR and proposed ePrivacy Regulation (currently under revision) include provisions which tackle some of the data protection challenges raised by the central role that personal data plays in digital advertising today, although they are not specific to advertising.

8.1.2.1 The effects of GDPR enforcement

Several data protection authorities have issued decisions which rule that some data processing practices that are widespread in the digital advertising industry are not compliant with the GDPR.

- In 2022, the Belgian data protection authority, the Autorité de protection des données (APD), found that the Transparency and Consent Framework (TCF), developed by IAB Europe, fails to comply with a number of provisions of the GDPR. The TCF underpins the way that data is shared and processed in real-time bidding (RTB), a standard used for programmatic display

⁹³¹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003 (COD) <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications>>.

advertising⁹³². This decision is linked to a complaint filed by several individuals and NGOs in 2019⁹³³. IAB Europe has submitted an action plan to the APD which “should enable a version of the TCF with a broader complaint functionality to be rolled out over a 6-month period under the supervision of the APD”. Meanwhile, IAB Europe has also filed an appeal against the APD’s decision which has led to the case being referred to the CJEU⁹³⁴.

- In 2021, the Norwegian data protection authority, Datatilsynet, found that Grindr was unlawfully sharing personal data with third parties for digital advertising purposes⁹³⁵, linked to a GDPR complaint filed by the Norwegian Consumer Council, Forbrukerrådet, in 2020. It has been reported that Grindr is appealing this decision on grounds that it “appears to want to hold Grindr – a relatively small player in a much larger ecosystem – responsible for industry-wide practices”⁹³⁶. The company also claims that the decision reflects “incorrect interpretations of the GDPR”⁹³⁷.
- In 2019, the French data protection authority, Commission Nationale Informatique et Libertés (CNIL), imposed a fine on Google for “lack of transparency, inadequate information and lack of valid consent”⁹³⁸ related to digital advertising, linked to a GDPR complaint filed by noyb and La Quadrature du Net in 2018. Although this decision was appealed by Google, the French Conseil d’Etat confirmed the ruling in June 2020. The Conseil

⁹³² ‘Decision on the Merits 21/2022 of 2 February 2022 Concerning: Complaint relating to Transparency & Consent Framework’ (*Autorité de protection des données*, 2021), <<https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>>.

⁹³³ Johnny Ryan, Pierre Dewitte, Jef Ausloos, Katarzyna Szymielewicz (with the NGO Panoptykon Foundation acting on her behalf), and the NGOs Bits of Freedom and Ligue des Droits de l’Homme.

⁹³⁴ ‘Case of IAB Europe against the Data Protection Authority 2022/AR/292’ (7 September 2022) <<https://www.gegevensbeschermingsautoriteit.be/publications/tussenarrest-van-7-september-2022-van-het-marktenhof-ar-292.pdf>>.

⁹³⁵ ‘Administrative Fine - Grindr LLC’ (*Datatilsynet*), <<https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/>>.

⁹³⁶ Fried I, ‘Exclusive: Grindr to Appeal Norwegian Fine for Privacy Violations’ (*Axios*, 14 February 2022) <<https://www.axios.com/2022/02/14/grindr-appeal-norwegian-fine-privacy>> accessed 8 September 2022

⁹³⁷ Fried I, ‘Exclusive: Grindr to Appeal Norwegian Fine for Privacy Violations’ (*Axios*, 14 February 2022) <<https://www.axios.com/2022/02/14/grindr-appeal-norwegian-fine-privacy>> accessed 8 September 2022

⁹³⁸ ‘The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC’ (*European Data Protection Board*, 21 January 2019) <https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en> accessed 8 September 2022.

d'Etat also did not allow Google to appeal the decision to the Court of Justice of the European Union (CJEU).⁹³⁹

- Additionally, several other complaints filed against Meta (covering Facebook, Instagram and WhatsApp) and Google are still being investigated by the Irish Data Protection Commissioner (DPC)⁹⁴⁰. This includes a complaint filed in 2020 relating to alleged infringement of rules on purpose limitation due to the way personal data is combined across different sites, apps and services owned by a digital advertising gatekeeper (Google)⁹⁴¹.
- However, to date, **there is little evidence that the regulatory action outlined above has led to significant changes to the structure and functioning of the digital advertising ecosystem as it pertains to personal data**. The GDPR may be a contributing factor to the industry's shift away from third-party data (see section 1) but **our research indicates that the volume and nature of personal data processing in digital advertising has not significantly changed** since the complaints related to these cases were filed between 2016-2020. There are several possible reasons for this.
- Firstly, GDPR complaints tend to focus on intermediaries or large platforms that earn a significant majority (in some cases, nearly all) of their revenue from processing personal data for digital advertising purposes. This gives those companies a strong incentive to resist legal and regulatory actions which could otherwise have a significant impact on their current business models. Such legal proceedings take time (usually, many years), allowing those platforms to persist with their processing until there is a final resolution of the case. Accordingly, most of the cases listed above remain unsettled. Much of the GDPR and related legal norms are untested by court or regulatory procedure. As a result, the true reach of the law is unknown. Platforms may therefore inevitably – and reasonably from their perspective – interpret the reach of the GDPR in restrictive ways which benefits their business models. For instance, the parameters of Article 2.2 GDPR are yet to be subject to any court or regulatory action.
- Secondly, the interviews for this study revealed that advertisers and publishers feel dependent on the large platforms which are at the centre of

⁹³⁹ 'Base de Jurisprudence - Decision N° 430810' (*Conseil d'État*, June 2020) <<https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/430810>>.

⁹⁴⁰ 'Annual Report 2021' (*Data Protection Commission*) <https://dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf> p. 57-64.

⁹⁴¹ Ryan J, 'Formal GDPR Complaint against Google's Internal Data Free-for-all' (*Brave*, 16 March 2020), <<https://brave.com/google-internal-data-free-for-all/>>.

some of these GDPR complaints to deliver and sell digital advertising, despite concerns about the legality of their data practices. **This dependency means that advertisers and publishers are likely to continue, in spite of their reservations, to invest in digital advertising tools which have been called into question, as long as they remain available on the market.**

- Thirdly, **in a market where the perceived value of using personal data is extremely high (see section 3), participants are unlikely to cease widely used data practices unless there is a clear legal imperative to do so.** Where decisions are being appealed, companies that are not the target of litigation (e.g. advertisers) are likely to consider there is a low risk of legal action against them for continuing existing practices, especially if there is a perception that “everyone else is doing it”.
- Additionally, several stakeholders interviewed for this study expressed the view that many of the harms outlined in section 2 persist because there has not been sufficient enforcement of the GDPR by data protection authorities in Member States, especially against Google and Meta. They argue that this is not a failure of the Regulation but merely of its enforcement. For example, the Irish Council for Civil Liberties (ICCL) has filed a lawsuit against the DPC accusing it of failing to enforce the GDPR with regards to Google’s digital advertising services.
- **Some data protection authorities interviewed for this study suggested that the complexity and lack of transparency of the digital advertising ecosystem is a barrier to effective GDPR enforcement, as significant resources and technical knowledge are required to effectively assess compliance in this context.** One significant example is the chain of different actors involved and the potential scope of those actors being “joint controllers” of personal data. That concept, of separate actors being jointly responsible for the “purpose and means of processing” on a complex data processing chain, is difficult to pin down in relation to the highly complex economic and technical relationships present within the digital advertising ecosystem. **The way that data is collected and used throughout this ecosystem is notoriously opaque (see section 1), resulting in difficulty establishing who has processed the data and who is responsible.** In turn, **the effort needed to establish the status of actors as controllers before ascertaining substantive breaches of the GDPR creates a significant hurdle for GDPR compliance and enforcement.** One advertiser interviewed for this study explained that “[our digital advertising] partners say they are GDPR compliant, but legal authorities say they are not [...] We have to work with these partners because they provide reach and impact, but they seem not

to fully comply with EU law. We want to stay compliant, so this is a major issue for us. **There is a “take it or leave it” approach when you try to negotiate contracts with them, creating a very unbalanced market dynamic**⁹⁴².

- In this context, while the GDPR provides a robust legal framework to regulate the processing of personal data, it appears that there may be some obstacles to GDPR enforcement due to the complexity and lack of transparency in the digital advertising ecosystem related to how personal data is collected and used. In addition, **the strong position and bargaining power of some large platforms means that the threat of legal non-compliance may not be a sufficient deterrent to advertisers and publishers to seek alternative options: while appeals are ongoing, current market practices are likely to persist until a final ruling has been handed down by the highest court (i.e. the CJEU) which could take several more years.** Given the shifts currently happening in the digital advertising ecosystem related to how personal data is collected and used (see section 1), the practices targeted by GDPR complaints which were launched as long ago as 2016 (see above) may have changed by the time these cases reach the CJEU, limiting the impact of such a ruling and requiring complainants and data protection authorities to launch new investigations on the latest technologies being used and tested by the digital advertising industry. This suggests that **GDPR enforcement needs to adapt to the rapidly changing and complex nature of personal data processing in a digital advertising context.**

8.1.2.2 The limits of the ePrivacy Directive with respect to fast evolving digital advertising

- The ePrivacy Directive has been used to challenge the validity of consent for digital advertising purposes in a number of cases, particularly in relation to “cookie banners”. In 2020, the French data protection authority CNIL fined Google €150 million for making it harder to refuse than accept cookies used to collect data for a number of purposes including digital advertising⁹⁴³. The CNIL also fined Amazon €35 million for placing advertising cookies on

⁹⁴² Advertiser 5.

⁹⁴³ ‘Délibération de La Formation Restreinte N°SAN-2021-023 Du 31 Décembre 2021 Concernant Les Sociétés Google LLC et Google Ireland Limited’ (*Commission Nationale de l’Informatique et des Libertés*, December 2021) <<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062>> accessed 9 September 2022.

the computers of users without prior consent or satisfactory information⁹⁴⁴. NGO noyb has launched more than 700 complaints related to cookie banners used to collect data for advertising purposes, linked to enforcement of the ePrivacy Directive⁹⁴⁵.

- The ePrivacy Directive has also been used to challenge large platforms' approach to applying a legal basis to their data collection practices linked to digital advertising. For example, in 2022 the Italian data protection authority issued TikTok with a warning that a proposed change to TikTok's privacy policy regarding the legal basis for digital advertising⁹⁴⁶ would infringe the ePrivacy Directive, highlighting the Directive's important role in regulating the collection of data using cookies and similar tracking technologies⁹⁴⁷. This led TikTok to suspend the planned change⁹⁴⁸.
- Although the ePrivacy Directive has successfully been used to regulate the way that many companies gather consent for cookies and other trackers that collect data for digital advertising, it is important to note that our research has indicated that the **digital advertising ecosystem is moving away from using cookies and other types of tracking technologies to collect data in the future**. The shift away from third-party data (see sections 1 and 5) is likely to lead to an increase in data collection through first-party methods which are not necessarily within the scope of the ePrivacy Directive (or the future ePrivacy Regulation), such as collecting data through logged-in user accounts (see section 1). These methods may not necessarily entail "the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user".⁹⁴⁹ **As the future landscape of data**

⁹⁴⁴ 'Cookies: The Council of State Confirms the 2020 Sanction Imposed by the CNIL against Amazon' (CNIL, 28 June 2022) <<https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon>> accessed 9 September 2022.

⁹⁴⁵ 'Cookie Banners' (noyb.eu) <<https://noyb.eu/en/project/cookie-banners>> accessed 9 September 2022.

⁹⁴⁶ To use legitimate interest as a legal basis instead of consent.

⁹⁴⁷ 'Provvedimento del 7 luglio 2022 [9788429]' (Garante per la Protezione dei Dati Personali, 7 July 2022) <<https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9788429>> accessed 9 September 2022; 'TikTok: Italian SA Warns against "personalised" Ads Based on Legitimate Interest' (European Data Protection Board, 15 July 2022) <https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads-based-legitimate-interest_en> accessed 9 September 2022.

⁹⁴⁸ 'Tik Tok rinvia la pubblicità basata sul legittimo interesse. Per il Garante privacy "una decisione responsabile"' (Garante per la Protezione dei Dati Personali, 12 July 2022) <<https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9789143>> accessed 9 September 2022.

⁹⁴⁹ Article 5(3) *ePrivacy Directive*: 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), OJ L201/37, <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>>.

collection in the digital advertising ecosystem evolves, there are concerns that the ePrivacy Directive (and future Regulation) may not remain future-proof in the context of new methods to identify and track users in a “cookie-less world”.

8.1.3 Transparency on environmental impact

- The large amount of data processing required to support the most widely used digital advertising methods leads to high energy consumption and emissions. One publisher did an internal study which found that 20 million impressions for a single ad resulted in about 2,200 kg of CO₂e. The information and communication technology (ICT) industry’s carbon footprint already represents approximately 4% of global greenhouse emissions⁹⁵⁰. Studies indicate that digital advertising represents a substantial proportion of these emissions⁹⁵¹.
- At the study workshop, one stakeholder suggested that most of the emissions from digital advertising come from “Scope 3” emissions (i.e. emissions generated by the supply chain used to deliver digital advertising). Another stakeholder argued that reducing the number of “middlemen” involved in the supply chain could lead to better yield optimisation for publishers and reduce emissions.
- Energy consumption and emissions related to digital advertising supply chains could be integrated in the proposed recast of the Energy Efficiency Directive regarding disclosure requirements of emissions from ICTs, especially data centres, by 2024⁹⁵² as well as a possible Union-wide sustainability rating scheme for data centres⁹⁵³. Large platforms may fall within the Article 11 Energy Efficiency Directive requirement that enterprises above a certain level of annual energy consumption implement an “energy management system” composed of elements such as the

⁹⁵⁰ Freitag C and others, ‘The Real Climate and Transformative Impact of ICT: A Critique of Estimates, Trends, and Regulations’ (2021) 2 Patterns

<<https://www.sciencedirect.com/science/article/pii/S2666389921001884>>.

⁹⁵¹ Pärssinen M and others, ‘Environmental Impact Assessment of Online Advertising’ (2018) 73 Environmental Impact Assessment Review 177

<<https://www.sciencedirect.com/science/article/pii/S0195925517303505>>.

⁹⁵² See Recital 66 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

⁹⁵³ Article 11 and 31 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

“monitoring of actual energy consumption, actions taken to increase energy efficiency, and measurement of progress”⁹⁵⁴.

- Several voluntary tools are in development which aim to enable individual companies to calculate and monitor the carbon footprint of their advertising campaigns⁹⁵⁵. However, stakeholders consulted for this study doubt whether a voluntary approach will be sufficient to address the considerable and growing environmental impact. **A clear requirement for all actors in the digital advertising supply chain to monitor the carbon footprint of advertising campaigns, based on a standardised measurement, could help drive awareness of the environmental impact of different advertising models and inform decisions about where ad spend is invested and how data is used. This could be combined with a reporting requirement for companies that spend or earn a significant amount of revenue on/from digital advertising to disclose on a periodic basis the volume of carbon emissions generated from digital advertising activities** in order to increase transparency at an industry level and improve understanding of the environmental impact of different advertising models. **A higher level of transparency in this context could also help inform future policy options, such as carbon emissions reduction targets for actors in the digital advertising supply chain.**
- **Certification could be developed for digital advertising models (or companies that offer these models), based on meeting minimum standards such as privacy safeguards, minimised environmental impact, transparency and security. Advertisers and publishers could be encouraged to use vendors that have been given this certification.** In the context of environmental impact, **certification could be used to point to compliance with Fit for 55 targets, such as the 45% renewable energy by 2030 target in the REPowerEU plan or the climate neutrality by 2050 target in the European Climate Law**⁹⁵⁶. Additionally, the EU taxonomy for sustainable activities could potentially be a useful vehicle for incentivising investment in alternative ad models. The taxonomy aims to provide companies with a set of definitions

⁹⁵⁴ Article 11 *Energy Efficiency Directive (recast)*: Proposal for a Directive of the European Parliament and of the Council on energy efficiency (recast), 2021/0203(COD).

⁹⁵⁵ See for example, methodology developed by Scope3 and the DIMPACT project: ‘About DIMPACT’ (*DIMPACT*) <<https://dimpact.org/about>> accessed 7 September 2022 and ‘Scope3 Methodology’ (*Scope3*) <<https://www.scope3.com/#Methodology>> accessed 7 September 2022.

⁹⁵⁶ *REPowerEU Plan*: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2022/230 final; *European Climate Law*: Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 (‘European Climate Law’), OJ L 243.

of “which economic activities can be considered environmentally sustainable” and could therefore clarify the environmental impacts of different models for the benefit of investors⁹⁵⁷, as well as advertisers, thereby incentivising the use of alternative models. **Including sustainable ad models in the taxonomy could also deter “greenwashing”, countering false or exaggerated claims of sustainability in the digital advertising ecosystem.**

- Various voluntary advertising industry initiatives⁹⁵⁸ have developed targets for the industry to reach net zero, as well as declaring support for UN initiatives such as the Race To Zero campaign⁹⁵⁹. It could be beneficial to explore ways to encourage and build on these initiatives, especially at EU level, as a way of incentivising industry actors to develop and implement alternative models which have been shown to reduce the environmental impact of digital advertising.

8.2 Allowing advertisers and publishers to know their audience

- In principle, advertising has always been ‘targeted’ to some extent, in the sense that marketers make rational decisions on segmenting and targeting before purchasing ad space. However, only recently has targeted advertising become associated with pervasive digital tracking and with ‘creepy’ or persistent ads over which individuals feel they have no control.
- The interviews conducted for this study indicated that advertisers and publishers want to be able to carry out responsible and proportionate data processing based on the trust of consumers in order to promote their products and services (advertisers) and generate revenue to fund the content they provide (publishers). However, the current structure of the market means that data provided to publishers or advertisers by individuals in the context of a trusted relationship is often shared with thousands of different intermediaries who also extract value from this data for ad targeting, profiling and measurement purposes. This is difficult for

⁹⁵⁷ ‘EU Taxonomy for Sustainable Activities’ (*European Commission*)

<https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en> accessed 8 September 2022.

⁹⁵⁸ Such as Ad Net Zero, initially developed in the UK and has now been adopted by industry associations in EU Member States such as Ireland and the WFA’s global initiative, Planet Pledge. ‘Advertising’s Response to the Climate Emergency’ (*Ad Net Zero*) <<https://adnetzero.com/>> accessed 7 September 2022; ‘Planet Pledge’ (*World Federation of Advertisers*) <<https://wfanet.org/leadership/planet-pledge>> accessed 9 September 2022.

⁹⁵⁹ ‘Race To Zero Campaign’ (*UNFCCC*) <<https://unfccc.int/climate-action/race-to-zero-campaign>> accessed 9 September 2022.

individuals to understand and control (see section 6) and it can create enormous amounts of waste, both from an economic and environmental perspective (see section 2).

- **Publishers raised concerns that their direct relationship with users means they are required to get consent for all of the data processing carried out by intermediaries in the digital advertising supply chain, even though the publisher itself often has limited transparency over what data these companies collect and how they process it. They are also concerned about “over-reliance” on consent and argue that legitimate interest could bring more certainty.**
- **This suggests that the data ecosystem which underpins digital advertising needs to become more balanced so that publishers and advertisers can generate value when individuals engage with their services and products in the context of trusted first-party relationships.** The data ecosystem also needs to become more accountable so that all actors involved in digital advertising can ensure compliance with the existing regulatory framework and restrict practices which exploit data in unethical ways that give rise to the harms outlined in section 2.
- From this perspective, and given the apparent lack of effectiveness of enforcement of the GDPR, so far, to address the issues in the digital advertising ecosystem in practice (see above) there is a need to consider how the general rules and principles of the GDPR address the specific issues related to digital advertising or could be further specified for this specific ecosystem.
 - Firstly, it could be considered whether or not the possibility of legitimate interest as a legal basis for advertisers and publishers to collect personal data from their customers for digital advertising purposes could be enshrined, subject to principles of proportionality and purpose limitation, in those limited circumstances where the advertiser or publisher has a direct relationship with the data subject.
 - Secondly, specific provisions could address the circumstances where there is no direct relationship between a company as data controller and a data subject, and where the data subject cannot be expected to be able to easily ascertain who is processing their data, and for what purposes, and is therefore unable, in practice, to exercise their rights. This appears to be the case with intermediaries in the digital advertising ecosystem. Therefore, it may be considered that such companies should not be entitled to be data controllers for the purposes of digital advertising, but that rather they should be limited

to the role of processors of personal data for the purposes of advertising, acting under the instructions of publishers or advertisers as controllers determining the objectives (serving an ad) and means of processing.

- Thirdly, where the company in question is a gatekeeper, there is likely to be a significant imbalance between them and the data subject, to the extent that the data subject is unlikely to be able effectively to exercise their rights. In these circumstances, the gatekeeper may restrict or prevent any third-party access to personal data, however the first-party processing of data may remain unclear and unaccountable from the perspective of the data subject, due to the imbalance between them. This may be evidenced in take-it-or-leave-it data policies which are frequently changed by the gatekeeper. Greater transparency about first-party data processing therefore appears insufficient as, without any further measures, it would simply transfer the burden onto data subjects to understand and decide whether to challenge the first-party data processing. **It would therefore be helpful to consider whether it is ever appropriate for gatekeepers in the digital advertising ecosystem to use consent as a legal basis to collect and process personal data for advertising purposes, given the potential imbalance of power between the data subject and gatekeeper. In this specific circumstance, further consideration would be needed as to whether it would be appropriate or proportionate to prohibit tracking for the purposes of advertising by gatekeepers.**
- The digital advertising ecosystem is moving away from reliance on third-party data collected by intermediaries due to moves by gatekeepers such as Google and Apple to limit third-party tracking in mobile and browser environments. This has given rise to the development of alternative digital advertising models (e.g. Privacy Sandbox, see section 5.2.1) which limit third-party tracking but nonetheless create opportunities for gatekeepers to exploit their ownership of essential services or access points (such as browsers and operating systems) to collect and monetise large amounts of user data. Publishers interviewed for this study explained that they feel they are unable to compete with these practices, because publishers only have the ability to collect data within the sites and apps where they distribute content.
- In addition, it is important to note that proposed provisions in the ePrivacy Regulation to enable consent to be expressed using technical settings of a

software application enabling access to the internet⁹⁶⁰ have been opposed by publishers and advertisers on the grounds that this will make it harder for them to collect first-party data from users of their websites in a transparent manner compared to large platforms like Google which have large numbers of logged-in users whose activities can be tracked without using cookies (and other trackers) regulated by the ePrivacy Directive (and future Regulation). Industry associations representing publishers and advertisers have in the past lobbied to preserve the ability for individual websites to display consent prompts to visitors.

8.3 Allowing consumers to choose whether and how to be targeted with ads

- In the current digital advertising ecosystem, buying and selling ads without the use of personal data is rare. Even the largely undefined notion of digital “contextual advertising” would likely require the processing of some personal data (for example, for measurement purposes), and would be a form of “targeted” advertising – as this method generally aims to target ads towards people who are likely to be interested in a specific product or service based on the content they are viewing.
- **In principle, advertising has always been “targeted”, in the sense that marketers make rational decisions on segmenting and targeting before purchasing ad space. However, only recently has targeted advertising become associated with pervasive digital tracking and with “creepy” or persistent ads over which the individual feels they have no control.** Action at Union level might be necessary to facilitate users’ ability to influence which ads they want to see online based on their own preferences, including the preference not to be targeted at all. This could be inspired by some of the principles in the EU’s Data Governance Act⁹⁶¹, which aim to increase trust in data sharing by establishing appropriate mechanisms for control by data subjects and data holders over data that relates to them.

⁹⁶⁰ Articles 9.2 and 10 of the Commission’s proposal for ePrivacy Regulation, *ePrivacy Regulation: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, 2017/0003 (COD) <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications>>.

⁹⁶¹ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ 2022 L 152/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>>.

- Such action would also complement Articles 26 and 39 DSA, which provide for enhanced transparency on targeting parameters. Article 24 DSA also provides for individuals to be informed about how to change parameters “where applicable”. However, the DSA does not impose any obligations to enable individuals to control or change these parameters if they want to.
- Article 25 DSA introduces provisions that prohibit providers of online platforms to “design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions”. It is possible that if this provision were applied to some of the ad settings tools reviewed in section 6, it could lead to improvements in user-friendliness. However, given that many of these tools provide individuals with choices about how their personal data is processed for digital advertising, it would be possible to argue that they would not fall within the scope of Article 25 DSA because practices covered by the GDPR and the ePrivacy Directive are specifically excluded⁹⁶².
- It is also important to note that Articles 25, 26 and 39 DSA only apply to providers of online platforms⁹⁶³ (Article 26 DSA) and very large online platforms⁹⁶⁴ and very large online search engines (Article 39 DSA). This means that these provisions would not necessarily apply to all ads displayed to individuals, for example ads displayed on a small news website.
- Key stakeholders in the digital advertising industry could be encouraged to address this by developing a single interface where individuals can easily indicate their preferences for data collection and targeting across the entire

⁹⁶² Article 25.2 DSA. 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹⁶³ Article 3(i) DSA defines an “online platform” as “a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.” 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

⁹⁶⁴ Article 33.1 DSA defines very large online platforms and very large online search engines as “online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to [Article 33.4].” 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), OJ 2022 L 277/1 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&qid=1666859140164&from=EN>>.

digital advertising ecosystem, for example through the establishment of a working group that involves industry, regulators and civil society.

- **This type of interface could give people the ability to create their own digital advertising profile, creating an “avatar” for ad targeting to be based on. People could also use this interface to “switch off” targeted ads altogether. From such a perspective, targeting could still be possible but based on trust and a less intrusive approach that minimises the processing of personal data.**
- This single interface could be made available in software settings or via a publicly accessible website and/or app. It could present individuals with different options related to how and when data is collected about them for digital advertising as they use their devices and online services. This could include (a) options to share certain categories of data (b) options to view and delete data used for ad targeting (c) options to opt in or out of all data collection for digital advertising. It could also, where technically possible, include options to share information proactively (e.g. currently planning a holiday in Greece). Preferences made via this interface should apply across the entire digital advertising ecosystem.
- Participation in the development of this interface should be encouraged from a wide range of non-industry stakeholders including civil society, academic experts and design professionals. An obligation for all companies that serve digital advertising to respect the preferences indicated via this interface could help ensure that individuals’ data protection rights are effectively respected.
- Such a development could be a step towards greater consumer empowerment in the digital advertising ecosystem, beyond the gains in transparency which are expected from the DSA.

The above recommendations are presented as a possible follow up to this study – whether in the form of further study or options for future policy interventions – in order to address the various and considerable issues which have been identified.

9 Conclusion

This study has collated evidence which on balance indicates a strong case to reform digital advertising. It indicates that the status quo is unsustainable, not only for individuals whose fundamental rights are undermined by the current model's focus on personal data, profiling and tracking, but also for publishers and advertisers who want to see more transparency and more competition in the digital advertising ecosystem. Advertising is currently a fundamental and legitimate part of the way internet services and content are funded; this study does not call that into question. However, digital advertising that relies on the collection of personal data, tracking of individuals and massive-scale profiling can have enormous unintended consequences. It undermines European citizens' data protection rights and can be linked to potential risks to security, democracy and the environment. Moreover, there is little independent evidence to support claims that the use of extensive tracking and profiling yields a significant advantage compared to digital advertising models which don't do this. There is, however, evidence to suggest that a proportion of advertising-related data collection and tracking could be unnecessary, fuelling ad fraud and 'made for advertising' websites that have limited value to society, as well as generating carbon emissions. The study's interviews with advertisers and publishers indicated that the digital advertising industry's current association with tracking and profiling has led to a race to the bottom, strengthening the position of players who have the most control over and insight into people's behaviour online and weakening the ability of other companies, especially advertisers and publishers, to communicate directly to their customers. This has created an accountability crisis in digital advertising, where individuals are expected to navigate a complex web of hundreds, if not thousands, of different companies in order to control the types of ads they see online.

The EU regulatory framework includes a variety of different measures that aim to tackle, to some extent, some of these issues. EU data protection regulation should provide individuals with a framework to prevent their personal data being collected and used for digital advertising purposes if they choose. Consumer law should prevent companies from misleading individuals into sharing more personal data than they wish for digital advertising. New instruments such as the Digital Services Act and the Digital Markets Act introduce provisions which could contribute to creating more transparency in digital advertising, both for businesses and individuals, but it is unclear that they will reduce incentives for large platforms and intermediaries to continue to track and profile individuals in order to generate revenue. However, this study points to gaps in the regulatory framework which could enable many of the issues highlighted in this study to persist. Overall, this study concludes that there is a need to improve transparency and accountability in the digital advertising ecosystem in three particular areas: ad spend and other

B2B issues (including ad measurement); the collection, use and dissemination of personal data; and environmental impacts. There is a need to increase individuals' control over how their personal data is used for digital advertising, including how they avoid unwanted targeting. There are also a number of obstacles that make it harder for advertisers and publishers to "know their audience" and communicate with them directly through advertising. This study recommends that these areas be the focus of future reflection and analysis, whether in the form of further research or options for future policy interventions, in order to address the various and considerable issues which have been identified.

Annex 1: Glossary

Ad exchange: Ad exchanges facilitate the buying and selling of advertising inventory by matching transactions between demand-side platforms (DSPs) and supply-side platforms (SSPs). They use real-time bidding (RTB) to determine the price of ad inventory according to the parameters set by both publishers and advertisers.

Ad network: Advertisers and publishers use ad networks to buy and sell display advertising (respectively). Ad networks can purchase ad inventory at a fixed price from publishers and sell it on to advertisers or do so using real-time bidding (RTB). Some ad networks may also buy inventory from supply-side platforms (SSPs) and sell inventory to demand-side platforms (DSPs).

Ad fraud: Ad fraud describes a wide set of activities that often aim to artificially inflate advertising revenue for a fraudulent actor. A typical form of ad fraud sees a limited number of servers generating a large amount of traffic, typically claiming to represent a large proportion of real individual users.

Advertiser: Advertisers are entities, including companies, that advertise their products and services via the digital advertising channels described in section 1.1.2.

Advertiser ad server: Advertisers and agencies use advertiser ad servers to store ads, deliver them to publishers, and measure and track the performance of campaigns.

Brand safety: Brand safety tools aim to limit the placement of ads next to content that might be harmful to a brand. They can exclude specific publisher sites (exclusion lists), restrict ad placements to specific publisher sites indicated by the advertiser or agency (inclusion lists); exclude (or include) only certain types or categories of publisher based on a range of criteria, exclude (or include) certain types of content based on criteria such as keywords and categories.

Contextual advertising: This term is used to describe digital advertising techniques that determine where an ad is placed based only on the content and environment in which it will be viewed⁹⁶⁵.

Cookie IDs: Cookies can be used to collect data about people's browsing history, including the websites and pages they visit and the content they view. Cookies

⁹⁶⁵ It is worth noting that contextual advertising can also be used in combination with digital advertising based on profiling.

are set by a server or directly by the websites that users visit and are stored in the user's browser.

Data management platforms (DMPs): Data management platforms (DMPs) allow advertisers, demand-side platforms (DSPs), supply-side platforms (SSPs) and publishers to manage and analyse their data, combine it with data provided by third parties, and create audiences that can be used for digital advertising based on profiling.

Demand-side platforms (DSPs): Demand-side platforms (DSPs) enable advertisers and agencies to automate the buying of digital advertising space from many sources.

Demographic data: Demographic data usually includes information about a person's gender, age, education level and income. However, some standard industry definitions of demographic data also include purchasing history and personal preferences⁹⁶⁶.

Digital advertising: This term is used to describe advertising which is served on a range of digital media, including websites, apps and connected devices such as smart TVs and audio platforms.

Digital advertising based on profiling: This term is used to describe digital advertising techniques that involve profiling⁹⁶⁷ of individuals in order to determine where an ad is placed⁹⁶⁸.

Disinformation: Disinformation refers to content, including ads, that intentionally spreads false information, often for financial or political gain.

⁹⁶⁶ See section 1.3.2.1 for a more detailed discussion of demographic data.

⁹⁶⁷ The GDPR defines profiling as "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements". *EU General Data Protection Regulation (GDPR): 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)*, OJ 2016 L 119/1.

⁹⁶⁸ Various studies and reports have described aspects of this type of advertising in many different ways, including "targeted advertising", "data-driven advertising", "personalised advertising", "surveillance advertising", "addressable media" and others. Many of these terms can be interpreted in different ways because they are not sufficiently precise about how they use personal data. "Targeted advertising", for example, could refer to advertising that uses personal data to decide how ads are targeted to individuals, but it could also refer to advertising which is targeted based on context without the use of any personal data.

Fingerprinting: Fingerprints are generated by combining attributes of the user's device or browser with data standardly provided in network requests (e.g. IP address, user agent string, operating system (OS) version). The permutation of these features is used to generate a hash which is used as an identifier and database key for that user.

Harmful content: In contrast to illegal content, harmful content refers to content that could be harmful to the individuals viewing, while not necessarily being illegal. This can include, for example, violent content, pornographic content, bullying and harassment content, and disinformation.

Identifiers: Identifiers enable different players in the advertising industry to re-identify individuals across contexts, platforms and devices. This requires a "join key" – a shared dimension between two data records that allows them to be connected.

Intent data: Intent data can be used to indicate whether an individual is actively considering the purchase or use of a product or service⁹⁶⁹.

Interest data: Companies can gain knowledge of individuals' interests based on observation of site and app interaction and usage. Examples may include content considered to be engaging for a user (e.g. read, liked, commented, shared), the groups a user is a member of (e.g. "second-hand luxury cars for sale in Luxembourg"), ads they interact with (e.g. viewed, clicked)⁹⁷⁰.

Intermediary: Advertisers, especially large ones, often work with a range of intermediaries to buy, sell and deliver advertising through different channels. These intermediaries are sometimes referred to as "ad tech" companies. The main types of intermediaries are demand-side platforms (DSPs), supply-side platforms (SSPs), ad exchanges, data management platforms (DMPs), ad networks and ad servers.

Large platform: Google and Meta earn advertising revenue both as publishers and providers of advertising technology services (intermediaries) in the programmatic supply chain. However, neither company publishes data about how much advertising revenue they earn as publishers compared to as intermediaries. This is why this study refers to Google and Meta separately as "large platforms".

Local profiling: Local profiling models use personal data about browsing behaviour stored on an individual's browser to determine where an ad is placed.

⁹⁶⁹ See section 1.3.2.3 for a more detailed discussion of intent data.

⁹⁷⁰ See section 1.3.2.2 for a more detailed discussion of interest data.

Measurement data: Measurement refers to the evaluation of the performance of digital ads. This can include, for example, whether or not an ad was viewed, how many people saw it, how many times an ad was shown to a particular person, and what actions were taken by the people that saw the ad⁹⁷¹.

Mobile IDs: Mobile devices have unique resettable mobile advertising identifiers (MAIDs). MAIDs are used to link data collected by an individual's phone to a specific individual. The MAID can then be used to identify, profile and segment people for advertising purposes. Data can be collected at operating system (OS) level or by apps.

Open display advertising: The part of the display market that sees a large range of publishers sell their inventory through a complex chain of intermediaries that run auctions on behalf of publishers and advertisers.

"Other" display: "Other" display advertising refers to display advertising on all websites and apps other than social media websites and search engines. It typically takes the form of display banner ads or video ads. The largest providers are primarily publishers such as broadcasters and online newspapers, along with large platforms that are not social media or search engine providers, such as Amazon.

Personal data: Under Article 4.1 General Data Protection Regulation (GDPR), personal data is "any information relating to an identified or identifiable natural person ('data subject')"⁹⁷².

Profiling: The General Data Protection Regulation (GDPR), describes profiling as "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements"⁹⁷³.

Programmatic advertising: Programmatic advertising is an overarching term used to refer to the automated buying and selling of digital ad space ("inventory").

⁹⁷¹ See section 1.3.2.5 for a more detailed discussion of measurement data.

⁹⁷² *EU General Data Protection Regulation (GDPR):* 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), OJ 2016 L 119/1.

⁹⁷³ *EU General Data Protection Regulation (GDPR):* 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), OJ 2016 L 119/1.

One common method, real-time bidding (RTB), sees advertisers compete for an impression by bidding in a real time auction as a website loads.

Publisher: The term “publisher” is often used in a digital advertising industry context to mean an entity that receives revenue from making advertising space available on websites, apps and other platforms that they own. This can include broadcasters, radio stations, newspapers, magazines, streaming platforms (e.g. Twitch), e-commerce sites (e.g. Amazon) and also large platforms such as Google and Meta (but see definition of “large platform” above).

Publisher ad server: Publishers use publisher ad servers to manage the sale of their ad inventory. They use them to set the decision logic underlying the ads served on their inventory based on bids they receive from supply-side platforms (SSPs) and through direct deals with advertisers.

Search advertising: Search advertising usually takes the form of advertising placed within a list of search results on a search engine website or app.

Social media advertising: Social media advertising typically either takes the form of in-feed ads (which blend in with content on the platform), display banner ads or video ads (e.g. before a video begins) placed on social media websites or apps.

Special category data: Special category data under Article 9 General Data Protection Regulation (GDPR) refers to personal data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”⁹⁷⁴.

Supply-side platforms: Supply-side platforms (SSPs) are used by publishers to manage, sell and optimise advertising space (also known as ad inventory) on their websites, mobile apps and other digital properties in an automated way. SSPs today also typically perform functions which used to sit separately under “ad exchanges”, namely facilitating the buying and selling of advertising inventory using auction-based systems to determine the price of inventory according to parameters set by publishers and advertisers.

Total display market: Should be understood as a combination of the “other” display market and the social media advertising market.

⁹⁷⁴ *EU General Data Protection Regulation (GDPR):* 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), OJ 2016 L 119/1.

User IDs: User accounts are used to identify individuals when they access a service (e.g. website, social media, apps). Verified user accounts unite an internal site/platform ID with a common identifier like an email address or telephone number, allowing data to be connected to an individual and used for advertising purposes.

Annex 2: Additional research areas

The drafting of this study highlighted several areas where further research could be beneficial.

For one, lack of transparency in the digital advertising ecosystem means that, in several important areas, data is either not available, not available at EU level or Member State level, or not provided by sources independent of the industry. For example, although the Spanish, French and UK competition authorities have conducted studies that provide a view into the structure of the market in those countries, much of the information that those studies contain is not available at EU level or for most EU Member States. That means that the availability of EU-level market share data is limited, making it more difficult to assess the relative importance of large platforms, intermediaries, and publishers. Further research in this area would make it easier to assess the extent of consolidation in the market and the experiences of large platforms' competitors. This would be particularly useful for the intermediary market, where the competitive landscape at Member State level is particularly opaque. More transparency into large platforms' different revenue streams (e.g. as intermediaries and as publishers), particularly at EU level, would also make it easier to assess the impact of policy interventions.

Although there is plenty of analysis of the impacts on privacy and data protection rights associated with digital advertising in the existing literature, there is generally a lack of quantitative and qualitative data describing their scale. For example, while there is evidence that the large data flows involved in the current digital advertising model come with security risks, there is no aggregate data on the number of cyberattacks that can be attributed to data leaked as a result of digital advertising practices. Additionally, while researchers have identified that digital advertising can be a vector for state surveillance, the full extent to which data used in digital advertising is the basis for this surveillance is unclear. Similarly, the possibility that digital ads can be used to manipulate vulnerable users and discriminate against certain groups has been identified by researchers but there is limited data available about the scale, which sectors are the most affected, or which types of manipulation and discrimination have the most negative impacts on individuals. Filling these gaps would make it easier to identify which of these impacts on privacy and data protection rights are the most severe and affect the most citizens, which could help inform appropriate policy responses.

Although the interviews undertaken as part of this study paint a relatively complete picture of advertisers' and publishers' experiences in digital advertising, further quantitative research into their experiences could be beneficial. For example, as highlighted in section 2, the amount of independent research into how much digital advertising based on profiling impacts publisher revenues

compared to other models is limited. Indeed, the amount of independent research into the effectiveness of the current digital advertising model based on profiling is generally scarce. Furthermore, the availability of quantitative research into which types of measurement data are most important to advertisers and publishers is limited and to what extent this contributes to campaign performance. Research in this area could help identify whether policy responses should consider specific types of measurement data which are seen to be essential to the effective functioning of the market. This would be particularly important in the context of policy designed to promote alternative models (given that different models imply different levels of access to measurement data). Similarly, more independent research into the effectiveness of large platforms' advertising services would be useful to shed light on whether advertisers' concerns (outlined in section 4) in this area are justified. Additionally, although industry research and the interviews undertaken as part of this study indicate that intermediary costs are high, there is little independent research into this topic. Further research and transparency into the pricing of intermediary services and digital advertising in general could be helpful especially when it comes to promoting the adoption of alternative models.

As highlighted in section 5, the amount of research that has so far been undertaken into alternative digital advertising models is limited, especially when it comes to sources independent from the industry. For example, areas where more quantitative research would be useful include how alternative models perform on key ad performance metrics (e.g. clicks, views and sales), their price in comparison to the current digital advertising model, their impact on publisher revenues, and the extent to which they can be used to prevent ads from appearing next to disinformation and harmful content. More independent research in these areas could help cater policy responses to promote their adoption as well as improve the industry's overall awareness of them.

Finally, although surveys exist that confirm the extent to which individuals are aware of the ad preference tools provided by Google, Meta, Apple and the European Interactive Digital Advertising Alliance (EDAA), few independent surveys have investigated whether individuals understand how to use these tools and their purpose. This would make it easier to assess the impact of specific design-choices associated with these tools.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696 or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

Open data from the EU

The EU Open Data Portal (<http://data.europa.eu/euodp/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

