Mapping online advertising issues, and the industry and regulatory initiatives aimed at addressing them

May 2020

Stephen Adshead, Yi Shen Chan, Tony Lavender, Laura Wilkinson, Aude Schoentgen

plumconsulting.co.uk

About Plum

Plum is an independent consulting firm, focused on the telecommunications, media, technology, and adjacent sectors. We apply extensive industry knowledge, consulting experience, and rigorous analysis to address challenges and opportunities across regulatory, radio spectrum, economic, commercial, and technology domains.

About this study

This is a study for the Department for Digital, Culture, Media & Sport on online advertising issues and self-regulatory initiatives. The research objectives are: (A) to assess the nature, scale and causes of harms arising from online advertising, and (B) to assess the current initiatives available to deal with these issues and to identify areas for improvement.

Plum Consulting
10 Fitzroy Square
London
W1T 5HP

T +44 20 7047 1919
E info@plumconsulting.co.uk

Contents

In brief 5

Executive summary 6

Online advertising issues 6
Scale of harmful advertising 7
Current regulatory initiatives 10
Effectiveness of the current system 11

1 Introduction 14

1.1 Terms of reference 14
1.2 Methodology 15
1.3 Caveats 16
1.4 Overview of the online advertising market 16
1.5 Structure of this report 18

2 Online advertising issues 19

3 Consumer issues 22

3.1 What is inappropriate advertising? 22
3.2 What is the scale of inappropriate advertising? 37
3.3 What are the economic and well-being impacts? 41
3.4 Participants and causal chain 44

4 Advertiser issues 55

4.1 Advertising fraud 55
4.2 Ad misplacement and brand risk 59

5 Regulatory framework 65

5.1 Legislation 65
5.2 The ASA and its role 66
5.3 Standards 67

6 Summary of industry and regulatory initiatives 68

6.1 Incentives and mechanisms of the current self-regulatory system 70

7 Industry standards and best practice 73

7.1 IAB Gold Standard 73
7.2 TAG Certified Against Malware programme 77

7.3 TAG Certified Against Fraud programme 79
7.4 JICWEBs Digital Trading Standards Group - brand safety 82
7.5 EDAA AdChoices 84

8 Platform rules and policies 91

8.1 Platform advertising policy scope 91
8.2 Policy enforcement 93

9 Technology solutions 94

9.1 Cybersecurity solutions 94
9.2 Distributed ledger technology 95

10 Consumer awareness campaigns 98

10.1 AA 'Media Smart' campaign 98
10.2 ICO 'Be Data Aware' campaign 100

11 Consumer tools and services 105

11.1 Ad settings on Facebook 105
11.2 Ad settings on Google 108
11.3 Web browser ad controls 113
11.4 Ad blockers 117

12 ASA initiatives 122

12.1 ASA avatars 2018 122
12.2 Emerging monitoring work 123
12.3 Engagement with platforms 124

13 Effectiveness of the current system 125

Appendix A Glossary 127

Appendix B Stakeholder engagement 130

Appendix C Examples of ad fraud 131

In brief

Online advertising is now the largest advertising medium by expenditure in the UK, exceeding TV and print. In 2019 it accounted for more than £13 billion expenditure in the UK and had a growth rate of 15% year on year.[1]

Online advertising involves various market segments. This study explores only the paid social display, open display and influencer marketing segments. Google and Facebook have strong market positions in the search/open display and social display advertising markets respectively, though there are a large number of other market participants, especially in the open display market.

As the online advertising market has grown, concerns around consumer- and advertiser-related issues have increased. The Advertising Standards Authority (ASA) received 16,059 complaints about online ads in 2018, 48% of all complaints and a 41% year on year increase.[2] Compared to other media, online advertising involves high volumes of ads, personalised targeting, computer code in ad creative, and a complex supply chain – these characteristics enable certain types of issues to occur that are not found in other media.

Consumer issues specific to online advertising include malicious ads, non-identified social media influencer ads, and harmful ad targeting. In addition, online ads may be offensive, misleading or otherwise harmful – these issues are not unique to online advertising but may be more prevalent online. There are also advertiser-related issues such as ad fraud and brand safety risk.

There is a lack of data about the scale of these issues due to limited detection and reporting, and limited sharing of data by market participants. However, case reports and the limited available data indicate that certain forms of harmful advertising are relatively widespread, especially malicious advertising.

Online advertising is subject to a system of self-regulation where the ASA plays the lead role in the enforcement of the CAP Code[3] through reputational sanctions and escalation to bodies with statutory powers in some advertising segments. The industry has also developed practices and initiatives to counter harmful advertising, including industry standards, platform policies, technology solutions, consumer tools and awareness campaigns. Many focus on advertiser issues of fraud and brand safety. Coordination around consumer issues, such as best practices in screening ads, is less well developed.

There are some gaps in the current system where there could be potential improvements including:

- Lack of a coherent consumer protection framework for online advertising issues,
- Need for better data for monitoring and to measure performance of the current regulatory system,
- Limited regulatory oversight of online platforms in terms of alignment of policies and guidelines with CAP Code provisions and agreed industry practices,
- Underdeveloped guidance around potential issues associated with targeting, such as discrimination and inappropriate targeting, and
- Limited scope and reach of consumer awareness and public education initiatives.

[1] IAB and PwC. Digital Adspend Study, 2018
[2] ASA and CAP. Annual Report, 2018.
[3] The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) is the rule book for non-broadcast advertisements, sales promotions and direct marketing communications (marketing communications).

Executive summary

This research study by Plum Consulting for the Department of Digital, Culture, Media & Sport (DCMS) covers the potential issues and areas of harm associated with online advertising. The two main objectives of the research are to: (a) develop further insight into these issues from the perspective of consumers and advertisers, and (b) examine the current efforts and initiatives by industry stakeholders to resolve issues.

The study was conducted mainly in February and March 2020, and this report provides a snapshot of the market and the associated consumer and advertiser issues at the time of writing. The online advertising market is characterised by a fast pace of change in terms of market structure, practices and competitive dynamics and is likely to evolve significantly over the next 6 to 12 months. The views expressed in this report are solely those of the authors. They are informed by findings of the research carried out by the study team and the team's previous experience and knowledge of the sector.

Online advertising issues

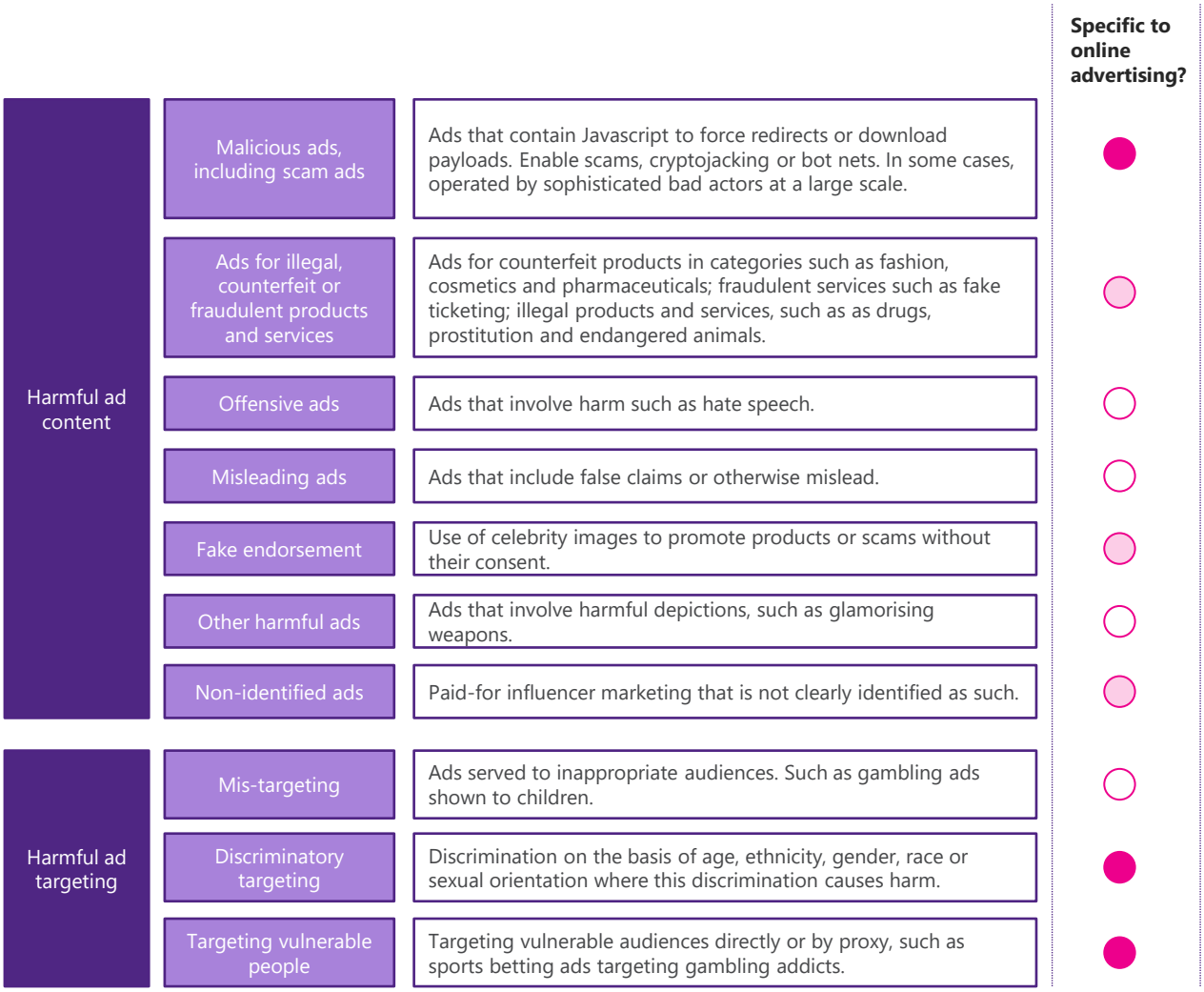
Online advertising experiences many of the same issues as advertising in print, television and other media, such as misleading claims and offensive ad content. But online advertising has a unique set of characteristics that enable certain of these issues to be exacerbated, or for other issues to occur. These characteristics include:

- **High volume of ads** – there are large numbers of online advertising campaigns, including a long tail of small-scale campaigns. There is potential for inappropriate advertising to occur and go unnoticed.
- **Personalised targeting** – in some cases, online advertising is targeted based on personal data, with potential for misuse of this data to target vulnerable people or to discriminate.
- **Computer code in ad creative** – online advertising creative includes not only images, animations or videos, but also computer code which can be misused to spread malware or for other malicious activity.
- **Intangible nature** – the act of an ad being served to a consumer device is intangible, leaving no record other than a data trail that is, in some cases, susceptible to misrepresentation or fraud.
- **Complex supply chain** – online display advertising is traded programmatically, involving a complex and relatively opaque supply chain, with potential for bad actors to perpetrate fraud or malicious advertising attacks.

The focus of this research is on paid-for advertising in the open online display market (advertising on publisher websites and apps), social display market (advertising on social media services) and influencer marketing (social media creators promoting products in return for payment). Advertising in search and classifieds, and commercial promotion in non-paid-for social media posts, brands' owned websites or apps, and on digital communications such as email are out of scope. Emphasis was placed on consumer-related issues and harms; advertiser-related issues are considered but these are a lower priority in this study.

Figure 1 shows a simplified segmentation of online advertising harms. Many of these categories are not unique to online advertising.

Figure 1: Segmentation of harmful advertising



Note: The categories are not mutually exclusive.

Scale of harmful advertising

There is some anecdotal evidence, such as press reports and complaints brought to the ASA, that these issues are relatively widespread. However, there is very limited data about the extent of harmful advertising that UK consumers are exposed to – and data that is available is not comparable.

Reasons for the lack of data include: (a) limited detection and measurement of inappropriate ads or fraud in the online advertising ecosystem; (b) limited data sharing by industry participants; (c) consumers might not notice inappropriate ads, especially in cases where the ad is subtly problematic, is inappropriately targeted (consumers

have limited visibility of how ads are targeted) or is hidden malware; and (d) consumers might not wish to report ads that they know are inappropriate or might not know how to.

Our findings on the scale of harmful advertising are summarised below.

- **Malicious advertising**. The proportion of UK online open display ad impressions that are malicious is estimated – very approximately - in the range 0.15%[4] to about 0.3%.[5] It is likely that hundreds of millions of programmatic display ads are served daily in the UK.[6] Therefore, hundreds of thousands of malicious ads may be served daily, affecting a significant number of UK consumers.

- **Illegal or counterfeit products and fraudulent services**. Paid-for online display advertising appears to be limited, with reports of harmful ads in this area referring to non-paid-for organic social posts.

- **Misleading, offensive and other harmful ads**. The vast majority of complaints received by the ASA relate to these categories of harmful ads. In 2019, the ASA received over 2,900 complaints relating to paid-for online advertising, excluding social media advertising.

- **Non-identified ads**. In 2019, the ASA received over 1,600 complaints about social influencers, mainly relating to the influencer not disclosing that the content was paid-for promotion.

- **Harmful targeting**. While there is anecdotal evidence of harmful targeting, for example ad campaigns that target specific vulnerable audience segments, there is little data available to establish the scale of such practices.

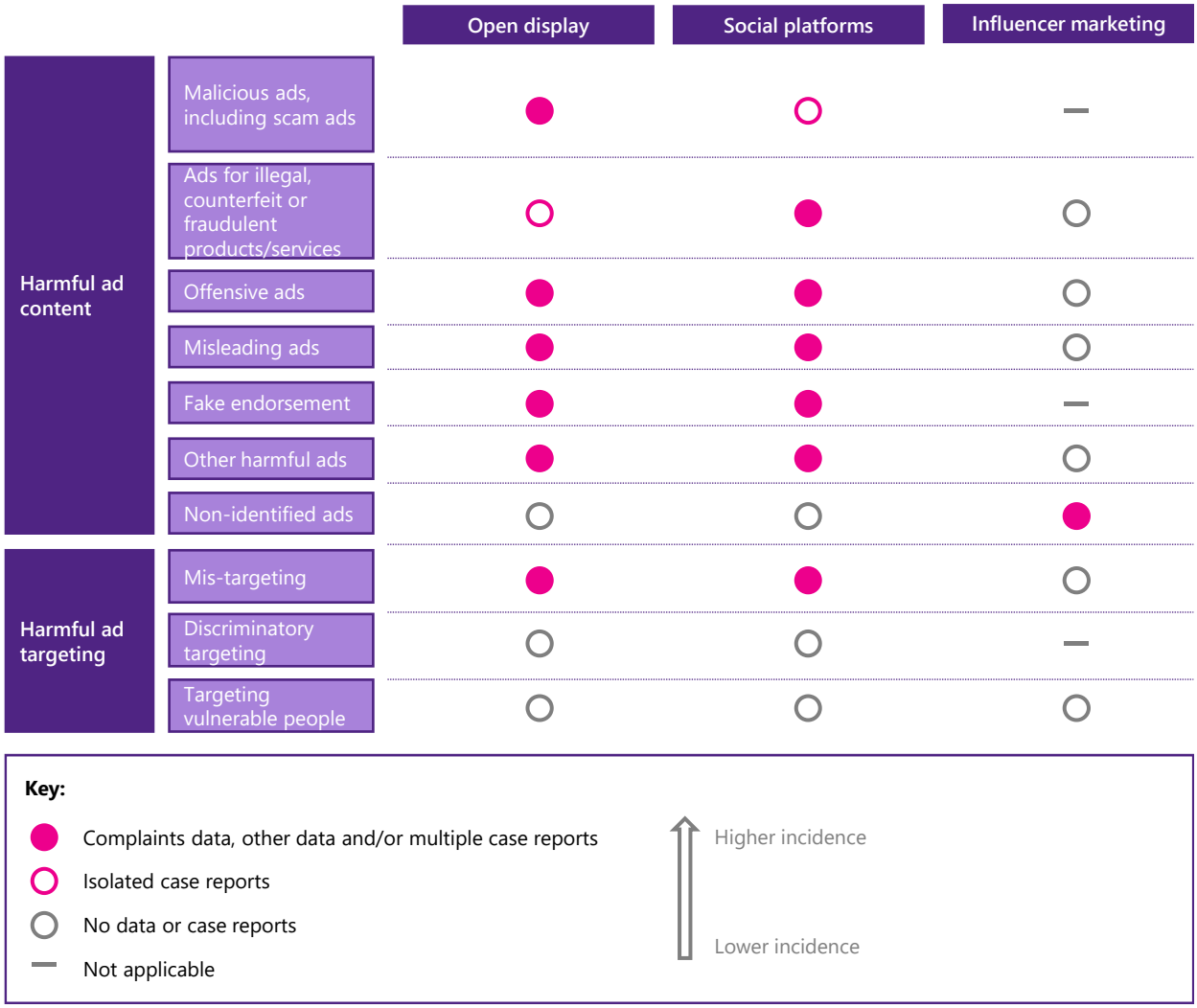
- **Ad fraud**. Estimates of the proportion of UK open display ad impressions that are fraudulent ranges from 0.53% in end-to-end optimised channels[7] (with fraud-prevention measures in place) to 11%[8] without optimisation. This data suggests that direct losses to ad fraud are in the range £5 million to £100 million in 2019.[9]

- **Brand safety risk**. The proportion of pages (content) that involve brand risk ranges from 2.8% (desktop display) to 9.8% (desktop video).[10] However, overreach of brand safety measures may cost UK news and magazine publishers £167 million annually in lost revenues.[11]

Figure 2 summarises the relative incidence of consumer-related harms in the online advertising segments considered in this study.

[4] Source: Confiant (2019). *Demand Quality Report, Q4 2019*.
[5] Source: Cybersecurity stakeholder interviewed for this project
[6] Plum Consulting estimate based on total programmatic ad spend and indicative CPMs.
[7] 614 Group (January 2019). *TAG European Fraud Benchmark Study*.
[8] Pixalate (2019). *Fraud Update*, Q2 2019.
[9] Plum Consulting estimate made by applying fraud rates to the size of the UK programmatic open display advertising market.
[10] IAS (2019). *Media Quality Report H1 2019*.
[11] University of Baltimore for Cheq, *The Economic Cost of Keyword Blacklists for Online Publishers*.

Figure 2: Relative incidence of harmful advertising in the UK



The scale of economic and well-being impacts will vary by the nature of the issues and the sectors affected. While there is limited quantitative evidence, one area where there are indicative figures on the economic impacts on consumers is malicious advertising associated with fraud and scams. The Home Office estimated that the total annual cost of fraud against individuals in England and Wales in 2015/16 was £4.7 billion.[12] More than three-quarters (76%) of fraud victims also reported that they were emotionally affected.[13]

We note from discussions with relevant stakeholders[14] that fraud cases in which online advertising is used as a means to lure in victims are on the rise. There are no specific figures on the volume of online advertising-related fraud. The Crime Survey for England and Wales (CSEW) [15] estimates that 3.7 million fraud incidents in the year ending December 2019, similar to the previous year.[16] In addition there are another 900,000 computer misuse offences experienced by the adult population over the same period.

[12] Home Office (23 July 2018). The economic and social costs of crime, second edition. Available at https://www.gov.uk/government/publications/the-economic-and-social-costs-of-crime
[13] Office of National Statistics (19 March 2020). Nature of crime: fraud and computer misuse. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse
[14] Such as the National Fraud Intelligence Bureau and technology vendors.
[15] Office of National Statistics (23 April 2020). Crime in England and Wales: year ending December 2019. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2019
[16] The CSEW also estimates that 54% of fraud incidents are cyber-related.

In other areas where online advertising may be linked to adverse socio-economic impacts, for example relating to exposure to restricted or illegal products and services such as alcohol, drugs, gambling and smoking, there are often multiple interrelated causes underlying the economic and social harms in these areas. While there is considerable research on the impacts on public health and well-being, evidence on the scale of harm in monetary terms that is directly associated with online advertising is scarce. In emerging areas of concern, such as mental health issues relating to the portrayal of body image and gender stereotypes in the media, online advertising is likely to be just one of a wide range of contributing factors. Such harms can also arise due to exposure to other forms of advertising (print and TV) as well as online content and social media use.

Current regulatory initiatives

There is a wide range of industry and regulatory initiatives and developments that contribute to mitigating the issues of inappropriate ad content, inappropriate ad targeting, ad fraud and brand safety risk. The mode of action of these initiatives ranges from provision of technology to enable the detection of malware, fraud and unsafe pages, through to industry standards that encode the use of this technology.

Consumer literacy campaigns educate the public about potential harms, while consumer tools and settings enable consumers to turn off certain forms of online advertising, encouraging the industry to deliver advertising consumers accept. ASA initiatives increasingly include proactive monitoring involving innovative technology-driven research techniques.

In many cases, the primary purpose of these initiatives is to address problems other than inappropriate advertising content and targeting, ad fraud or brand safety, and the impact on these issues is incidental. In addition, the reach and adoption of initiatives differs considerably, with self-regulatory schemes such as DTSG[17] Brand Safety relatively widely adopted, while TAG Certified Against Malware has lower adoption. There is limited evidence about the efficacy of these initiatives, and some are likely to have only a low impact on the issues in scope of this study. Figure 3 provides a summary of the key industry initiatives.

[17] Digital Trading Standards Group (DTSG).

Figure 3: Issues addressed by industry and regulatory initiatives

Category	Initiative / development	Issues addressed				
		Malvertising	Bad content	Bad targeting	Ad fraud	Brand safety
1. Industry standards and best practice	IAB Gold Standard				●	●
	TAG Certified Against Malware	●				
	TAG Certified Against Fraud				●	
	JICWEBs DTSG brand safety					●
	EDAA AdChoices		○	○		
2. Platform rules and policies	Various	●	●	●		
3. Technology solutions	Cybersecurity solutions	●	●		●	●
	Distributed ledger technology	○			○	
4. Consumer media literacy campaigns	AA Media Smart		○	○		
	ICO Be Data Aware			○		
5. Consumer tools and services	Service settings/features			○		
	Browser ad controls			○		
	Ad blockers	○	○	○		
6. ASA monitoring and best practice initiatives	ASA Avatars			●		
	Emerging ASA initiatives	●	●	●		

Key:
● Initiative specifically directed at solving or mitigating the issue.
○ Initiative has an impact on the issue, but it was established to address other problems/issues

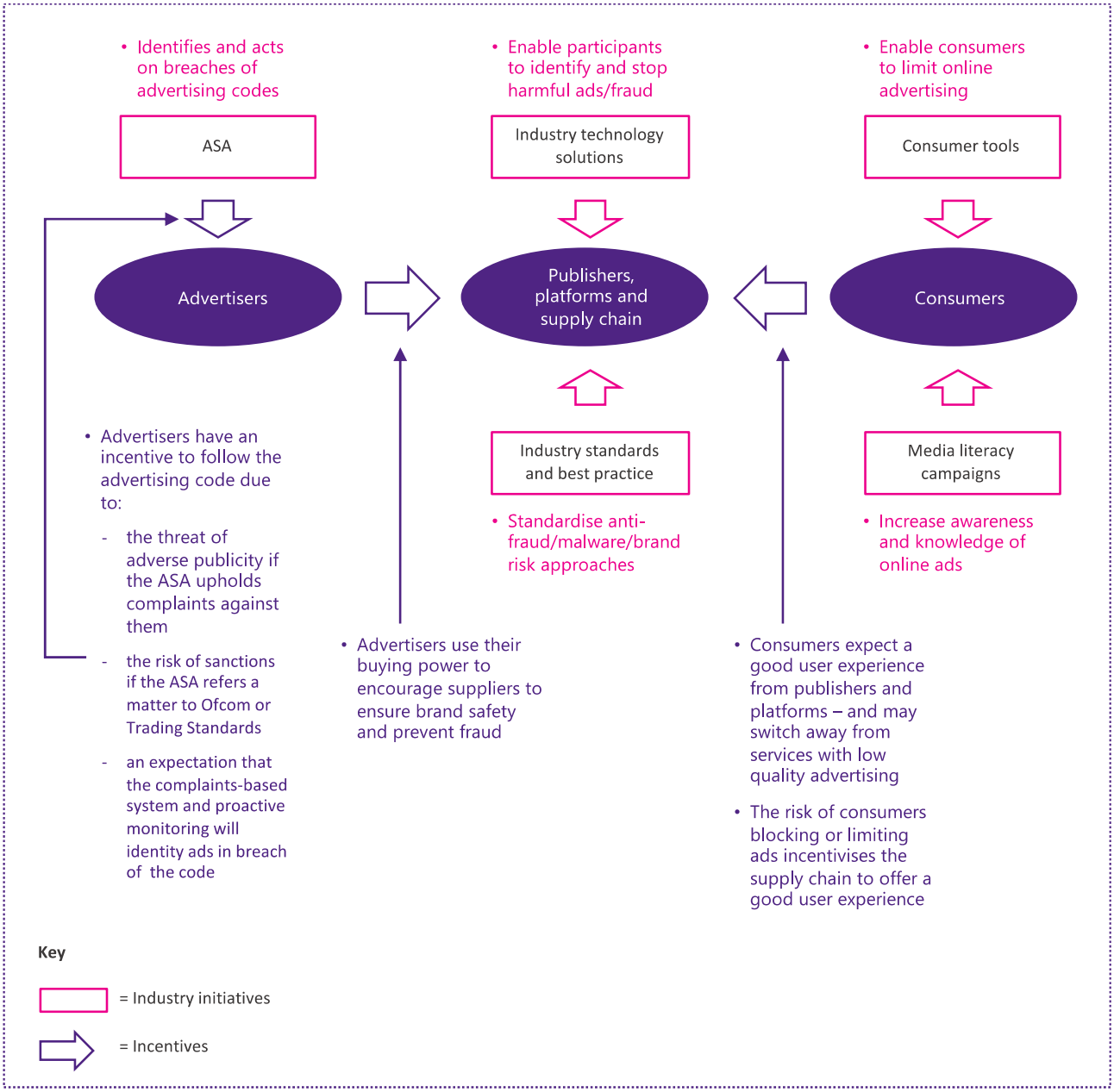
Effectiveness of the current system

The current self-regulatory system is based on a set of incentives for market participants to comply,[18] and a set of industry bodies, initiatives and market developments to support and encourage compliance with industry standards across a range of advertising issues. Figure 4 illustrates this system. At a high level:

- Advertisers are incentivised to comply for reputational reasons – to avoid the risk of brand damage from running inappropriate advertising and being caught out.
- The supply chain – including agencies, social media platforms, open display market intermediaries and publishers – is incentivised by pressure from its advertiser and consumer customers.
  - Advertisers want to prevent brand risk and fraud. They can, to some extent, use the threat of switching suppliers to exert this pressure.
  - Consumers want a good user experience and quality advertising. In cases where they have a choice of publisher or platform, they may favour services that provide a good experience. In addition, they may limit online advertising by using an ad blocker or changing service settings.

[18] For example, in the case of CAP Code regulation

Figure 4: Online advertising self-regulatory system



The effectiveness of self-regulation depends crucially on the incentives to participate. In the online environment the emergence of new forms of data-driven advertising and social media has introduced a host of new players across a complex ecosystem, and as mentioned above, the incentives for these players may not be aligned along common interests. For instance, bad actors intent on causing harm through malicious advertising have little or no incentive to abide by industry standards and CAP Code regulations. In the growing social influencer segment, individual influencers may be less aware of potential issues and may not see the need to abide by the relevant guidelines.

The risk is that consumers may not receive adequate protection in a self-regulatory system which potentially leaves some industry players unregulated. In this regard, we identify the following areas for improvement.

- Lack of a coherent consumer-protection framework for online advertising issues. There are two related aspects to this.

  - First, there is room for a more coordinated and clearly signposted mechanism for consumers to report inappropriate advertising and to help consumers understand the available options and process for redress. At present, there is a confusing patchwork of reporting methods and this makes it difficult for consumers seeking redress.[19]

  - Second, there are overlaps in regulatory structure and responsibilities which makes enforcement potentially difficult and time consuming. Various agencies with different and overlapping remits have an interest in the online advertising sector;[20] and no one single organisation has all the necessary expertise, information and/or powers to effectively address some of the areas of harm identified. This is a fast-evolving industry where issues can emerge and change. Also, the nature and causes of some of these harms go beyond just online advertising[21] which underlines the need for closer coordination between regulatory agencies to improve regulatory efficiency and effectiveness.

- Better data for monitoring purposes. Other than ASA complaints data, there is no easy way to monitor and measure the performance of the self-regulatory system. More data sharing, ideally in a standardised format, by players in the online advertising value chain with the relevant agencies will help promote accountability and transparency.[22] We note also that the ASA, as a self-regulatory entity, does not have information-gathering powers which are underpinned by legislation and this is an area which may require cooperation with other agencies with an interest in the sector.

- Limited regulatory oversight of online platforms. The CAP Code applies to advertisers but not online platforms. We note that these platforms have detailed policies and guidelines on advertising and general online content which are generally aligned with the CAP Code and industry agreed practices. However, there could be more clarity on how these policies and guidelines are enforced and whether they have had significant impacts on the issues they are meant to address.

- Limitations of the incentive-based system. Major advertisers and platforms are held to account by concerns around their reputation and, in the case of advertisers, their ability to continue advertising. These incentives hold less sway over overseas advertisers, short-term advertisers and bad actors.

- Underdeveloped guidance around potential issues associated with targeting, such as discrimination and inappropriate targeting. Presently, the main codification of rules is around the mis-targeting of advertising to children. This could be an area for further investigation.

- Limited scope and reach of consumer awareness and public education initiatives. Expanding these programmes can help raise awareness of online advertising issues and the available tools and options to address some of them. We note that the ASA and advertising industry have identified raising public awareness as part of their strategies.[23,24]

[19] The nature of harms varies and affect consumers in different ways and complaints can be made through various channels such as the ASA, Trading Standards, Citizens Advice and Action Fraud, as well as through online platforms, such as Facebook, Google and Instagram.
[20] These include the ASA, Action Fraud/National Fraud Intelligence Bureau, Citizens Advice, CMA, ICO and Trading Standards.
[21] Related to this is a definitional issue – online advertising overlap with online content, for example in the area of organic social media posts which are not covered by the ASA. It is clear that some areas of consumer harms in online advertising are also associated with online content more generally. Activities to protect consumers and the wider public in the online environment may need to take both aspects into account.
[22] The retention of ads will allow analysis of past activities and trends, and may be a possible option to consider.
[23] ASA (1 November 2018). More Impact Online: the ASA's 2019-2023 Strategy. Available at https://www.asa.org.uk/uploads/assets/uploaded/96455868-e7b1-4ac7-8185f37893fd6f0d.pdf
[24] Advertising Association (March 2019). Arresting the Decline of Public Trust in UK Advertising. Available at https://www.iabuk.com/sites/default/files/public_files/AA_Public_Trust_Paper.pdf

1 Introduction

In 2018 the Department of Digital, Culture, Media & Sport (DCMS) commissioned a research report by Plum Consulting that explores the structure of the online advertising sector, including the movement of data, content and money through the online advertising supply chain.[25] It also assesses the potential for harms to arise as a result of the structure and operation of the sector – these include harms to consumers such as fraud and scams, harms to businesses such as advertising fraud and brand reputation, and wider social issues arising from exposure to inappropriate advertising and discriminatory targeting.

This study builds on the findings from that report and seeks to (a) develop further insight into the online advertising issues from the perspective of consumers and advertisers, and (b) examine the current efforts and initiatives by industry stakeholders to resolve issues.

1.1 Terms of reference

The DCMS has commissioned this study on online advertising issues and self-regulation with the following two objectives:

1. To further quantify and qualify the issues associated with online advertising and the associated drivers, through a rapid evidence review; and

2. To explore to what extent market forces, consumers, self and co-regulation initiatives are able to address these issues, and to identify areas where solutions need further development or areas where initiatives have not yet been introduced.

The issues covered by this study include:

- Consumer exposure to fraudulent and scam-based advertising;
- Consumer exposure to misleading and harmful advertising;
- Consumers being targeted inappropriately;
- Advertiser-related issues such as ad misplacement, brand safety risk and ad fraud; and
- Consumers, advertising businesses and regulators' ability to identify when online advertising rules have been broken and pursue recourse.

In examining the above topics, the focus is more on emerging issues in the online advertising sector and less on areas where the regulatory guidelines are fairly well-established such as for alcohol, gambling and food and drinks which are high in fat, salt or sugar (HFSS). Emphasis was placed on consumer-related issues and harms; advertiser-related issues are considered but these are a lower priority in this study.

1.1.1 Categories of advertising in scope

The DCMS defined the scope of this research to include paid-for advertising in the open online display market (advertising on publisher websites and apps), social display market (advertising on social media services) and

[25] Plum Consulting (January 2019). Online Advertising in the UK: A report commissioned by the Department for Digital, Culture, Media & Sport. Available at https://plumconsulting.co.uk/online-advertising-in-the-uk/

influencer marketing (social media creators promoting products in return for payment). Advertising in search and classifieds, and commercial promotion in non-paid-for social media posts, brands' owned websites or apps, and on digital communications such as email are out of scope[26]. The scope of this study is narrower than the ASA's remit, which includes search, organic social and claims made on advertiser websites and apps.

Figure 1.1: Scope of this study relative to the ASA's remit

Category	Description	In scope of the study	Within the ASA's remit
Paid search	Paid-for listing in search results, such as sponsored or promoted listings.		✓
Paid social display	Range of paid-for advertising formats on social media platforms.	✓	✓
Organic social	Advertiser posts/content on social media platforms – not paid for.		✓
Open display	Banner, video and native ads and sponsored content on publisher services.	✓	✓
Classifieds	Paid listings such as recruitment, property, cars and services.		✓
Influencer marketing	Paid promotion on creators' social media posts.	✓	✓
Email marketing	Content in advertiser email marketing and paid-for advertising in third-party newsletters.		✓
Advertiser websites and apps	Content on advertiser websites and apps, such as a retailer ecommerce website.		✓

The focus is on the UK market, though the report also provides international data and examples where UK-specific data or insight is limited.

1.2 Methodology

The research involved desk research and stakeholder interviews, including the following activities which were mainly carried out in February and March 2020.

- Review of industry reports, trade publications, company websites and reports, reports by government or regulatory agencies[27] and relevant academic literature.
- Interviews with industry stakeholders to gather insights and views on the issues associated with online advertising and the current state of regulatory initiatives. These included industry bodies such as the Advertising Standards Authority (ASA), online platforms, publishers and cybersecurity solutions vendors. Further information on the stakeholders who contributed to this research is provided in Appendix B.

[26] The remit of the Advertising Standards Authority (ASA) includes non-paid online advertising as well as paid advertising. For more details on the ASA's remit under the Committee of Advertising Practice (CAP) Code, see https://www.asa.org.uk/advice-online/remit-general.html

[27] Such as the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Centre for Data Ethics and Innovation (CDEI) and Ofcom.

Where possible, we also sought to gather data from the stakeholders interviewed to supplement the desk research.

1.3 Caveats

We present a snapshot of the market and the associated consumer and advertiser issues at the time of writing. The online advertising market is characterised by a fast pace of change in terms of market structure, practices and competitive dynamics and is likely to evolve significantly over the next 6 to 12 months.

While the research scope focuses on online open display and social display paid-for advertising, some of the consumer-related harms covered in this report also occur across other forms of online advertising (e.g. search and classified) as well as through other forms of online communications (e.g. organic or non-paid advertising on company websites or social media posts), and may indeed be more prevalent in these other areas.

Furthermore, the discussion of some types of consumer harms (e.g. negative impacts on well-being such as on mental health) related to online advertising also needs to be considered in the wider context of harms associated with user behaviour and exposure to the general online and social media environment, beyond just online advertising.

We were unable to gather substantial data from stakeholders to supplement our analysis. The study period coincided with the outbreak of the Covid-19 crisis in the UK which led to delays and some difficulties in the industry engagement exercise. Most of the stakeholders approached for this study were cooperative and we were able to arrange to speak to them but most of the views and information provided were qualitative in nature and limited quantitative evidence was provided.

The views expressed in this report are solely ours. They are informed by findings of our research and our previous experience and knowledge of the sector.

1.4 Overview of the online advertising market

The UK online advertising market generated expenditure of £13 billion in 2018[28] and comprises three main market segments: search, display (social and open) and classifieds. This study explores issues in the £5.1 billion online display advertising market, as well as influencer marketing, which is likely to account for revenue of the order of £200 million.[29]

The social display market segment involves Facebook, YouTube and other social media platforms providing advertising on their owned and operated services. They are vertically integrated across the supply chain, providing functions from self-service sales interfaces and auctions, through to ad serving. They hold consumer data in closed "walled gardens".

In contrast, the open display market segment involves a complex ecosystem of intermediaries (see Figure 1.2) that cooperate to enable programmatic (automated) trading, and data-driven targeting. Importantly, open display market practices are likely to change when Google Chrome phases out third-party cookies by 2022.

[28] Source: CMA (December 2019). Online platforms and digital advertising, Market study interim report.
[29] Source: Spark Ninety estimate, 2019.

Figure 1.2: Programmatic online advertising supply chain – simplified[30]

In influencer marketing, social media creators promote products in return for payment, generally brokered by specialist agencies or platforms. Targeting is relatively broad.

Figure 1.3: Segmentation of the UK online advertising market

Market segment	Description	Examples of providers	Ad spend, 2018[31]
Search	Paid-for listing in search results, such as sponsored or promoted listings.	Google, Bing	£5,821 million
Social display	Range of advertising formats on social media platforms.	Facebook, Instagram, YouTube, Snapchat, Twitter, LinkedIn, TikTok	£3,044 million
Open display	Banner, video and native ads and sponsored content on publisher services.	The Guardian, Reach, Mail Online, ITV, Channel 4, Buzzfeed	£2,205 million
Classifieds	Paid listings such as recruitment, property, cars and services.	Gumtree, Autotrader, Zoopla, Monster	£1,470 million
Influencer marketing	Paid promotion on creators' social media posts.	Social media influencers	£200 million *

Notes:

= In scope

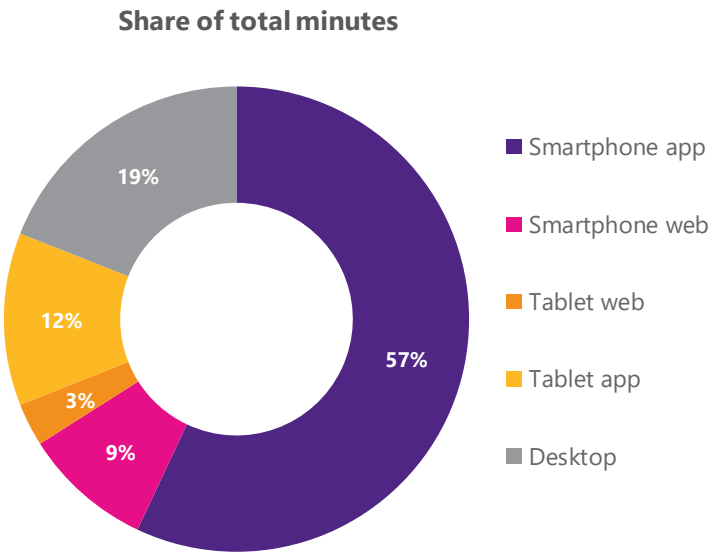
= Out of scope

* = Highly approximate estimate

The consumption of online services is increasingly on mobile devices (smartphones and tablets) and via apps. Figure 1.4 shows the share of total UK minutes by device and platform (web or app). In December 2019, smartphones and tablets accounted for 81% of online minutes, with desktop only 19%. Apps accounted for 77% of online minutes.[32] In 2018, smartphones accounted for 51% of total digital ad spend.[33]

[30] Spark Ninety. (January 2020). Transparency in programmatic online display advertising markets: Presentation to the 6th meeting of the expert group for the European Commission Observatory on the Online Platform Economy.
[31] Sources: IAB / PwC Digital Adspend Study, 2018. Spark Ninety estimate – influencer marketing.
[32] Source: Comscore (December 2019). MMX Multi Platform, Age 18+, UK
[33] Source: IAB / PwC Digital Adspend Study, 2018

Figure 1.4: Online minutes by device and web vs. app, UK adults, December 2019



Source: Comscore MMX Multi Platform

1.5 Structure of this report

The rest of this report is structured as follows.

Section 2 provides an overview of the nature, scale and causes of online advertising issues.

Section 3 describes the various consumer issues and potential harms arising from online advertising.

Section 4 describes the advertiser issues and potential harms associated with advertising fraud, and ad misplacement and brand safety.

Section 5 describes the regulatory framework which governs the online advertising sector and the different bodies involved and their roles.

Section 6 summarises the current status of industry and regulatory initiatives and this is followed by the assessment of different categories of initiatives, namely:

- Industry standards and best practice in **Section 7**,
- Technology solutions in **Section 8**,
- Consumer awareness campaigns in **Section 9**,
- Consumer tools and services in **Section 10**, and
- ASA initiatives in **Section 11**.

Section 12 provides our findings on the effectiveness of the current regulatory system and identifies gaps where solutions need further development and areas which may require further study.

2 Online advertising issues

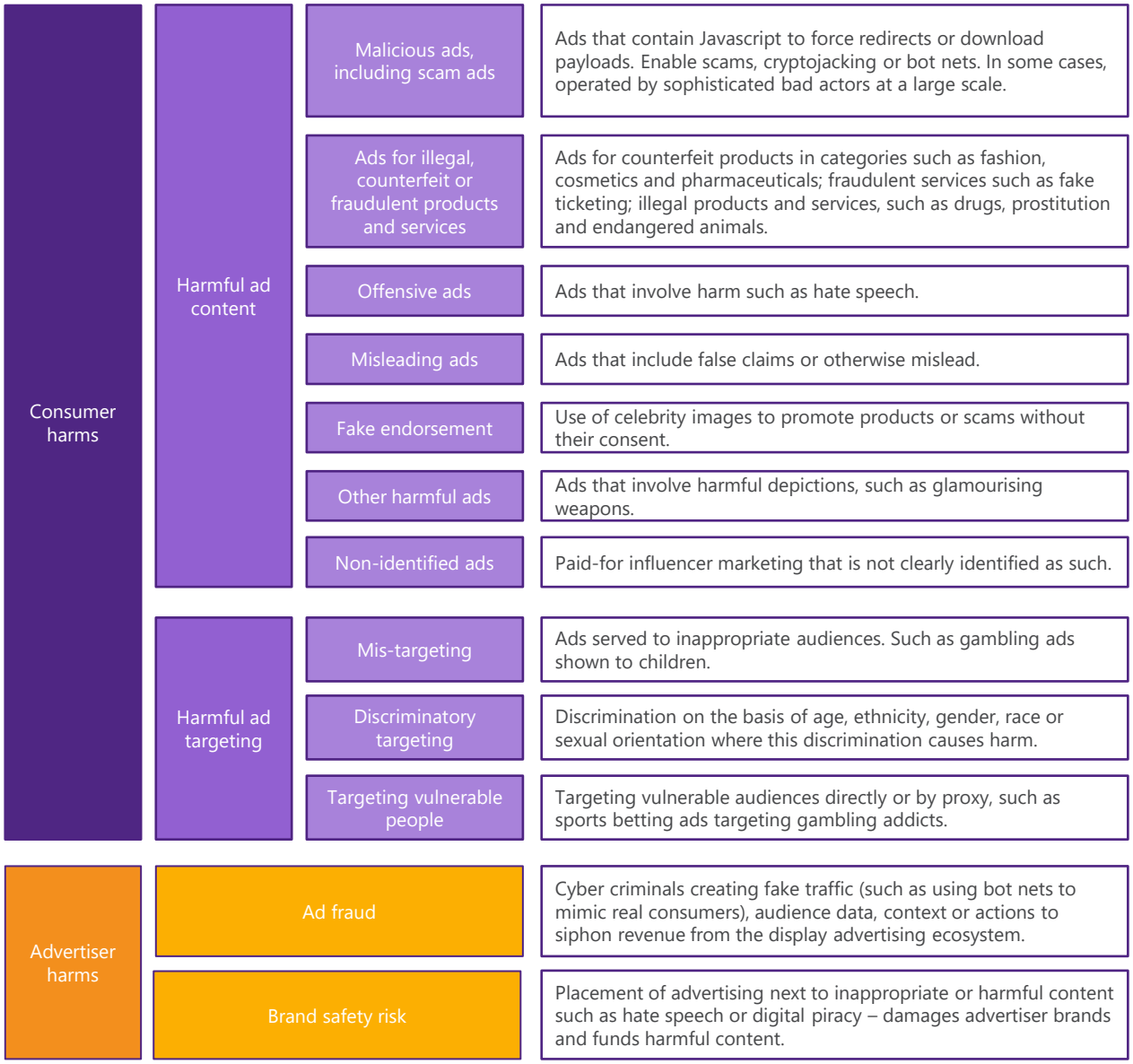
Online advertising experiences many of the same issues as advertising in print, television, radio and other media, such as misleading claims and offensive ad content. But online advertising has a unique set of characteristics that enable certain of these issues to be exacerbated, or for other issues to occur. These characteristics include:

- High volume of ads – there are large numbers of online advertising campaigns, including a long tail of small-scale campaigns and dynamic creative campaigns in which an individual sees a tailored variant of an ad. In these cases, there is very limited shared audience for each ad, with potential for inappropriate advertising to occur and go unnoticed.
- Personalised targeting – in some cases, online advertising is targeted based on personal data, with potential for misuse of this data to target vulnerable people, possibly bombarding them with advertising, or to discriminate.
- Computer code in ad creative – online advertising creative includes not only images, animations or videos, but also computer code which can be misused to spread malware or for other malicious activity.
- Intangible nature – the act of an ad being served to a consumer device is intangible, leaving no record other than a data trail that is, in some cases, susceptible to misrepresentation or fraud.
- Complex supply chain – online display advertising is traded programmatically, involving a complex and relatively opaque supply chain, with potential for bad actors to perpetrate fraud or malicious advertising attacks.

These characteristics may combine to exacerbate harm. A lack of a detailed public record of advertising and the small scale of some advertising campaigns may mean that harmful ads go unnoticed and/or it is challenging to determine the extent of exposure to harmful ads that are identified.

Figure 2.1 shows a simplified segmentation of online advertising harms according to whether consumers or advertisers are the primary victims of harm, and the category of issue. Issues that are specific to online advertising or exacerbated in online advertising are highlighted.

Figure 2.1: Segmentation of harmful advertising



Note: The categories are not mutually exclusive.

The focus of this study is on the harms associated with online advertising. It should be noted that there is recent work by the Centre for Data Ethics and Innovation (CDEI) on online targeting,[34] as well as ongoing work by the Information Commissioner's Office (ICO) on the use of personal data within the adtech industry,[35] and by the Competition and Markets Authority (CMA) looking into competition issues and market power associated with online platforms and digital advertising in the UK.[36] This study has sought to steer clear of the areas covered by these other bodies though there is inevitably some overlap. For example:

[34] CDEI (4 February 2020). Review of online targeting. Available at https://www.gov.uk/government/publications/cdei-review-of-online-targeting
[35] ICO (17 January 2020). Blog: Adtech - the reform of real time bidding has started and will continue. Available at https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/
[36] CMA. (18 December 2019). Online platforms and digital advertising market study. Interim Report. Available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

1. For some areas of harm, online advertising is a contributing factor but there are also other factors that are relevant such as non-advertising online content or communications; and

2. Some of the potential underlying causes of some of the online advertising issues may be due to the market structure of the online advertising sector where digital platforms such as Google and Facebook have market power in certain key parts of the value chain.

The following sections set out, for consumer issues then advertiser issues:

- What the issue is;
- The scale of the issue in terms of advertising affected;
- Economic and well-being impacts; and
- The causes and drivers of the issue.

3 Consumer issues

Summary

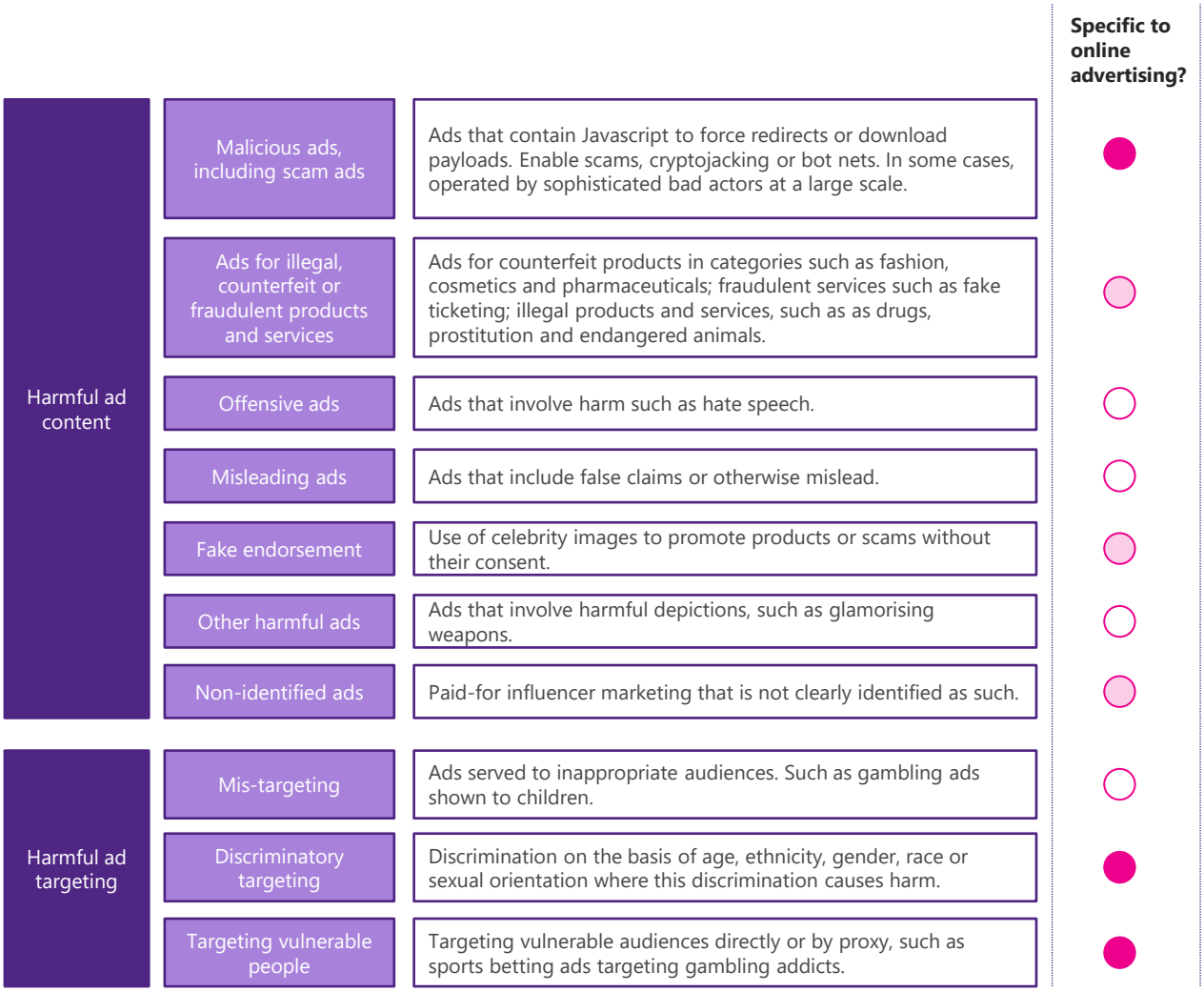
Nature:	Various categories of inappropriate ad content and ad targeting from scam ads to offensive ads.
Scale:	There is very limited data about consumer exposure to inappropriate ads.
Market:	Open display advertising, social display advertising and influencer marketing.
Victims:	Consumers.
Impact:	Varies according to type of ad from mild offence to significant financial loss.
Instigators:	Bad actors (malicious ads, ads for illegal products) and legitimate advertisers (other ads).
Causes:	Includes the presence of bad actors, some legitimate advertisers not following rules, limited controls in the supply chain, difficulty with timely reporting, and market complexity.

3.1 What is inappropriate advertising?

Online advertising may be harmful to consumers if the advertising is for a scam or inappropriate product or service; the content of the ad is harmful or offensive; the ad is misleading; or the ad is otherwise non-compliant with the CAP Code. Online advertising may also be harmful if it is targeted in a discriminatory way, to vulnerable groups or to inappropriate audiences. Figure 3.1 below, shows the main categories of inappropriate advertising. This segmentation is not intended to be exhaustive, given that the CAP Code includes a large number of highly detailed rules for advertising generally, and for a specific range of product and service categories.

Inappropriate targeting and malicious ads are specific to online advertising, enabled by the technological capabilities of the online advertising ecosystem – addressable targeting and Javascript in ad creative, respectively. Advertising for counterfeit goods and illegal and restricted products has developed in tandem with online trading of these products. Misleading ads, offensive and harmful ads, and ads that do not follow CAP rules in other areas are not unique to online advertising and also occur in other media such as television and print. In print and on television, each ad is generally seen by a mass audience and there is a record of this ad. However, online advertising can be finely targeted, with each ad potentially seen by a small audience or, in the case of dynamic creative, an individual, without a public record of this advertising. In consequence, it is challenging to determine the extent of consumer exposure to harmful advertising.

Figure 3.1: Categories of inappropriate advertising



3.1.1 Malicious ads

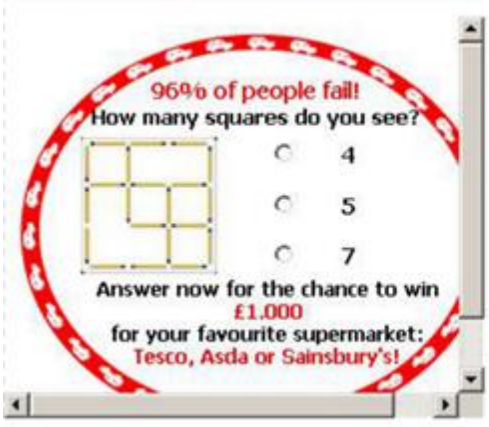
In online display advertising, the content of an ad is distributed in an electronic file known as the creative. In many cases of malicious ads, bad actors insert Javascript code into this creative file for malicious purposes. This code may initiate a forced redirect – sending the user's browser to a malicious web page – or load additional payloads, such as malicious pop-up ads. Generally, the purpose of these tactics is to force users to view and interact with content enticing them to take part in scams. Malicious advertising is unique to online advertising.

These scams are generally perpetrated by organised cyber-criminals and often involve phishing – a fraudulent attempt to obtain sensitive information, such as usernames, passwords or credit card details. Typical examples include fake system security alert notices ('Your PC is infected with 3 viruses … enter your details to fix the

problem') and fake prizes ('You have won an iPhone … enter your details to claim this prize'). Figure 3.2 shows an example of malicious phishing advertising that was run in the UK in the weeks leading up to the 2019 General Election, with attacks doubling in a week. The fraudulent sweepstake pop-up (1) was placed via an online advertising intermediary. Users who clicked on this pop-up were redirected to another pop-up (2) that asked for their personal information (gender, age) and thoughts on supermarket pricing and value. The Media Trust determined that the unauthorised phishing was the main purpose of this ad.[37]

Figure 3.2: Example of malicious pop-up ads used for phishing

(1) Sweepstake pop-up



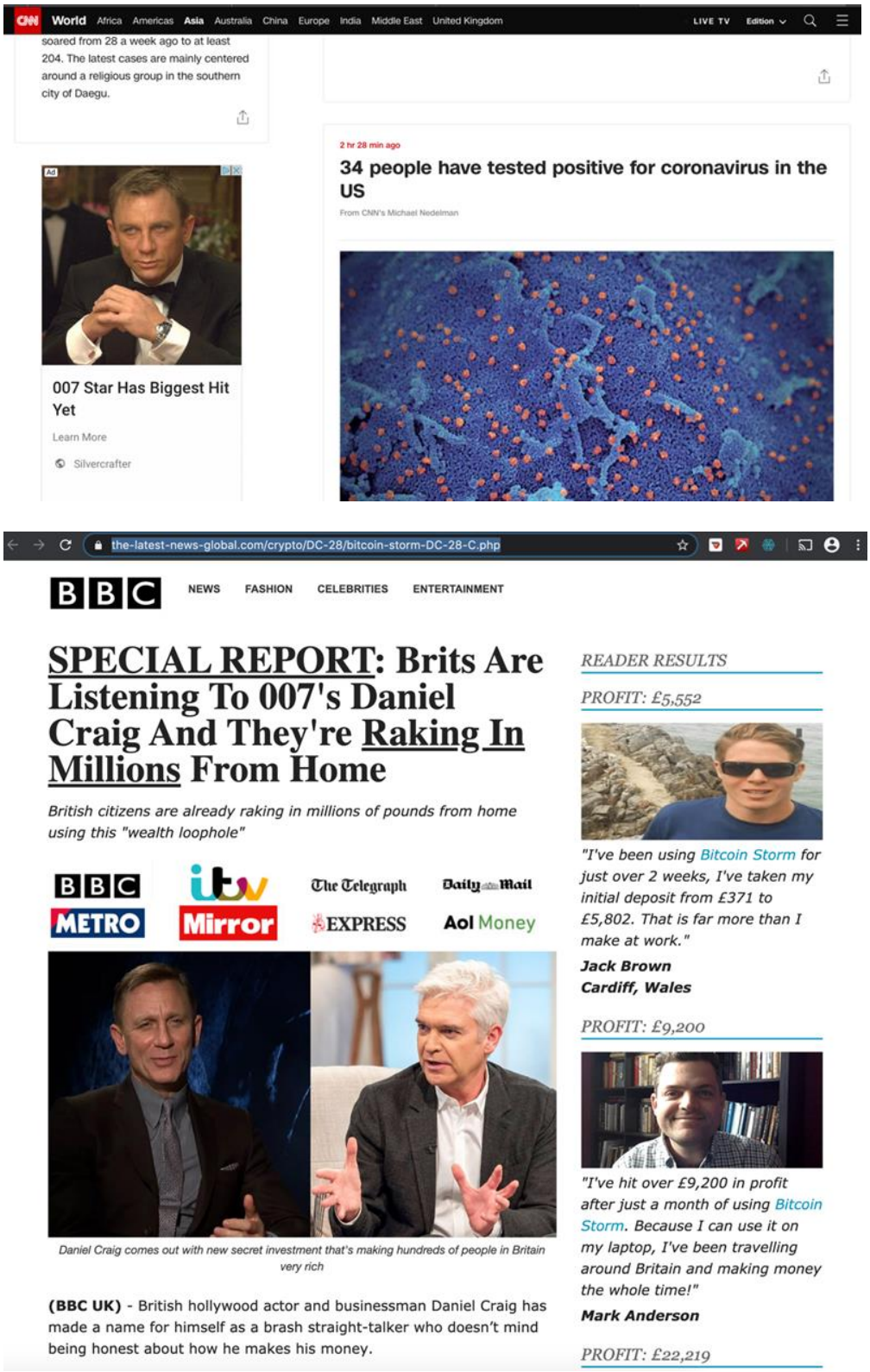
(2) Phishing pop-up

Source: The Media Trust

Some scams do not use forced redirects, but celebrity clickbait images on ads to encourage users to click through to malicious scam web pages such as fake news stories about scam investment schemes. They use cloaking techniques to disguise these malicious landing pages from ad tech vendors' screening systems. Figure 3.3 shows an example of a celebrity clickbait ad identified on the website of CNN. A reader clicking through on the ad will be redirected to a landing page of a fake BBC News page which advertises a bitcoin scam.

[37] The Media Trust, *Malvertising spikes during UK national elections*.

Figure 3.3: Daniel Craig clickbait advertisement on CNN website



Source: Plum Consulting[38]

[38] The project team accessed the CNN web page and clicked from the ad through to the fake BBC news page on 21 February 2020 and reported the scam ad to CNN and to Google via its implementation of the Ad Choices interstitial. This example was picked up during the project team's day-to-

As the Covid-19 pandemic has developed, fraudsters have adapted the celebrity clickbait used in malicious advertising campaigns. In April 2020, ads appeared claiming that Martin Lewis had died which clicked through to scams.[39]

In other cases, ads carrying malicious Javascript may infect the user's device with malware which, in some cases, operates as part of a botnet. These botnets may be used for malicious purposes such as:

- Generating fake advertising impressions as part of ad frauds (see Section 4.1). In 2018, the US Department of Justice announced that it had dismantled two international cybercriminal rings and indicted eight defendants for causing tens of millions of dollars in losses in digital advertising fraud. The fraudsters used malicious advertising to infect at least 1.7 million Windows computers with malware creating a botnet that was involved in creating fake advertising impressions[40].

- Cryptojacking – using a device's resources to "mine" forms of online money known as cryptocurrencies without the user's permission. In 2018, Spotad detected malware related to mining of the cryptocurrency Monero on seemingly legitimate desktop and mobile ads,[41] and malicious code was discovered in display advertising on YouTube.[42]

These infections of a user's device are a criminal offence under the UK's Computer Misuse Act 1990. There is very limited data about the extent of these issues (see section 3.2), especially the relative scale of ad fraud, cryptojacking and other activities enabled by malicious advertising.

Malicious advertising may occur on both desktop and mobile devices. Many reported examples of malicious ads are in the open online display advertising ecosystem, though an investment scam is reported to have used "fake ads" on Facebook to attract victims.[43]

3.1.2 Ads for counterfeit goods and fraudulent services

Advertising may be for counterfeit goods or fraudulent services, ranging from fraudulent ticketing, dating and financial services, to the sale of counterfeit goods. However, we did not find substantial evidence that such occurrences are common in the open online display market and the social display market. These issues appear to be more common in search advertising and organic social media marketing.[44]

This category excludes cases where malicious Javascript in the ad is used to cloak the URL of the fraudulent advertiser – included in Section 3.1.1 above. Advertising for counterfeit or fraudulent goods and services is not unique to online advertising, but is likely to be more prevalent online due to the large number of ads and advertisers involved.

There is a large online retail market for counterfeit goods, such as fashion, cosmetics and pharmaceuticals. In many cases, these counterfeit goods are being advertised through online display advertising. The problem is particularly prevalent in influencer-centric online commerce and on social media platforms such as Facebook and Instagram. For example, it is estimated that in 2019 there were some 57,000 counterfeit accounts active on

day web and app usage. The scope of the project did not involve conducting a systematic review of publisher web content for inappropriate advertising. In consequence, we did not determine how rates of malicious advertising on CNN and Google (as an intermediary) compare to other publishers and intermediaries, respectively. It is possible that this example of a malicious ad was distributed on various other publishers and intermediaries as well as CNN and Google.

[39] https://www.thesun.co.uk/money/11452204/martin-lewis-warns-coronavirus-scammers-dead/

[40] https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing

[41] https://www.coindesk.com/crypto-malware-miners-israel-ad-networks-monero

[42] https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/

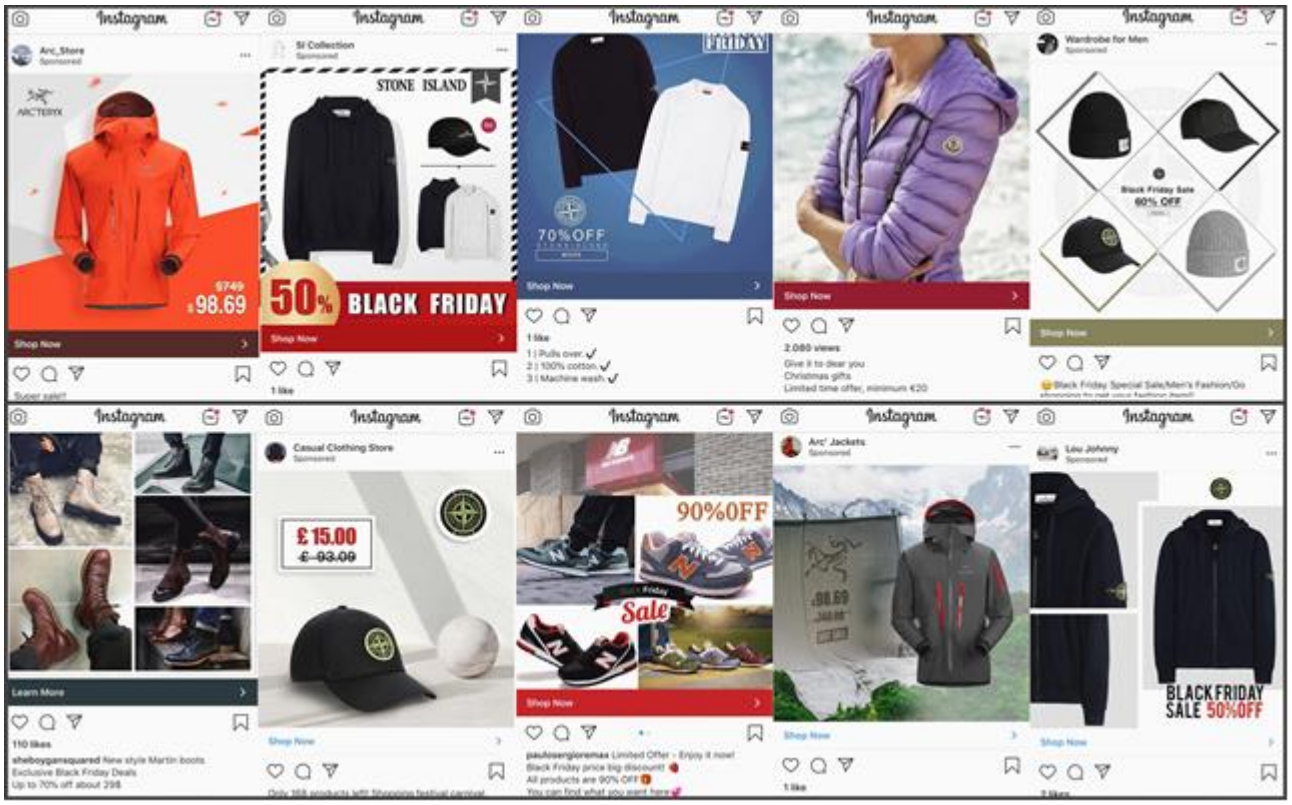
[43] https://www.theguardian.com/world/2020/mar/01/revealed-fake-traders-allegedly-prey-on-victims-in-global-investment-scam

[44] For example, an investigation by *The Times* revealed that fraudsters are making use of Facebook fan pages of pop stars to offer fake or non-existent tickets and asking those interested to send them direct messages. Source: The Times (16 March 2019). Fans' fury over Facebook ticket scam. https://www.thetimes.co.uk/article/fans-fury-over-facebook-ticket-scam-v8x6pn60w

Instagram which are responsible for 15.5% of posts published on the hashtag timelines of fashion brands.[45] In some cases, these accounts run paid-for advertising campaigns – some examples are illustrated in Figure 3.4.

Besides using social media platforms to market their goods, counterfeit sellers also make use of communication tools, such as WhatsApp and WeChat as a means of communicating to potential buyers. In some cases, they also set up external websites to display and sell their products. Often these replicate the look and feel of a legitimate brand's website.

Figure 3.4: Examples of Instagram ads marketing counterfeit goods



Source: World Trademark Review[46]

3.1.3 Ads for illegal or restricted products and services

Online advertising may promote products or services that are illegal or restricted in the UK. These include drugs, guns, prostitution, endangered animals, human body parts and human trafficking. Note that not all instances of these products or services are illegal.[47] The use of the internet and social media platforms for marketing such products and services is likely to be prevalent as identified in various studies, for example, drugs,[48] endangered wildlife[49] and adult services.[50] An example of paid-for online advertising for such products is social media ads by

[45] Ghost Data (April 2019). Instagram and counterfeiting in 2019: new features, old problems. Available at ,https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf
[46] https://www.worldtrademarkreview.com/anti-counterfeiting/black-friday-fakes-instagram-urged-verify-advertisers-counterfeits-problem
[47] For instance, the provision of adult services in itself is not illegal.
[48] Volteface (September 2019). DM for Details: selling drugs in the age of social media. Available at https://volteface.me/app/uploads/2020/03/DM-for-Details-I-Volteface.pdf
[49] International Fund for Animal Welfare (IFAW) (May 2018). Disrupt: Wildlife Cybercrime. Available at https://www.ifaw.org/resources/Disrupt%20Wildlife%20Crime%20PDF
[50] All-Party Parliamentary Group (May 2018). Behind Closed Doors: Organised sexual exploitation in England and Wales. Available at https://appgprostitution.uk/wp-content/uploads/2018/05/Behind-closed-doors-APPG-on-Prostitution.pdf

beauty salons and clinics for Botox injections which are prescription-only medicines and thus cannot be advertised to the public.[51]

Advertising for illegal or restricted products and services take place through various avenues including paid-for advertising, classified ads, discussion forums and other marketing means on social media platforms, such as direct messaging, social media posts, groups, videos or 'stories'. The examples from the existing literature and recent studies suggests that the promotion of such products and services, especially those which are unambiguously illegal, tends to be through other forms of online advertising or organic social media marketing.[52]

The actors behind such advertising can range from legitimate businesses which may not be aware of the legal status regarding such products (e.g. beauty clinics advertising Botox) to individual actors and organised criminal groups who are less likely to make use of paid-for open display advertising to market these products and services.

3.1.4 Offensive ads

The content of online advertising may cause harm or offence if it contains violence, adult content, gore or otherwise shocking material. The CAP Code also warns against ads that cause offence on the grounds of race, religion, gender, sexual orientation, disability or age.[53] Offensive advertising is not specific to online advertising and also occurs on other media, such as television, radio and print.

An example is the ad campaign by betting company Paddy Power ahead of the 2017 boxing fight between Floyd Mayweather and Conor McGregor. The ASA ruled that the ad was "likely to cause serious offence on the grounds of race" and thus breaching rule 4.1 of the CAP Code on Harm and Offence.[54] The ads had run in the London Evening Standard and the Metro newspapers. Paddy Power was ordered to remove the ad from the internet.

Figure 3.5: Paddy Power ad ruled to be offensive by the ASA

Source: BBC article, 20 September 2017[55]

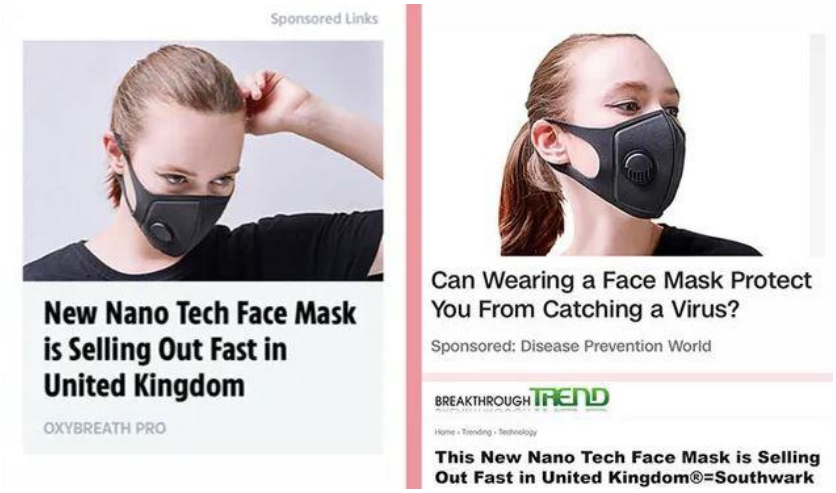
[51] https://www.asa.org.uk/resource/enforcement-notice-botox-social-media.html
[52] For example see Volteface report on sale of drugs on social media.
[53] CAP Code, 4: Harm and Offence. Marketers should take account of the prevailing standards in society and the context in which a marketing communication is likely to appear to minimise the risk of causing harm or serious or widespread offence.
[54] https://www.asa.org.uk/rulings/power-leisure-bookmakers-ltd-a17-397121.html
[55] https://www.bbc.co.uk/news/uk-41330470

3.1.5 Misleading ads

Online advertising may be misleading if it includes false or unsubstantiated claims, incorrect information, omissions or any of a wide range of other misleading information. The CAP Code includes thorough rules on misleading advertising which make up the majority of concerns tackled by the ASA. Misleading advertising is not specific to online advertising and also occurs on other media, such as television, radio and print.

One example is a series of paid-for display ads by an advertiser based in Estonia for a particular brand of face mask which were seen via the Taboola and Outbrain networks on the Scottish Sun and CNN websites in February 2020 as shown in Figure 3.6. The ads had linked to landing pages which contained articles referencing the coronavirus health crisis and how facemasks are selling out, alongside information on attributes of the face mask in question.

Figure 3.6: Misleading face mask ads banned by the ASA



Source: Huffpost article, 4 March 2020[56]

The ASA challenged whether the ads were misleading, irresponsible and scaremongering. In its assessment, the ASA pointed out the alarmist language used, and the repeated references to high demand for the masks and the likelihood of stock selling out quickly were intended to exploit people's fears regarding the coronavirus outbreak. Noting that Public Health England did not (at the time) recommend the use of face masks as a means of protection from coronavirus, the ASA thus found that the ads were misleading, irresponsible and likely to cause fear without justifiable reason.[57] The ads were judged to be in breach of CAP Code rules 1.3 (Social responsibility), 3.1 (Misleading advertising) and 4.2 (Harm & offence).

3.1.6 Unapproved celebrity endorsements

The CAP Code states that endorsements must be genuine.[58] In some online ads they are not. This practice is common in malicious advertising for scams, as illustrated in Section 3.1.1 with the example of Daniel Craig. Genuine businesses have also used celebrity images to misleadingly imply endorsement. Unapproved endorsement appears to be relatively specific to online advertising.

[56] https://www.huffingtonpost.co.uk/entry/face-masks-ads-banned-coronavirus_uk_5e5e3b4dc5b6732f50e80df4
[57] https://www.asa.org.uk/rulings/novads-ou-cas-599611-h1h2q1.html
[58] CAP Code: 3.45 Marketers must hold documentary evidence that a testimonial or endorsement used in a marketing communication is genuine, unless it is obviously fictitious, and hold contact details for the person who, or organisation that, gives it.

In February and March 2017, Sterling Partnership Ltd placed a paid-for Facebook ad that included an image of Martin Lewis and text which stated "Get the Latest Money Saving Tips & Advice" as shown in Figure 3.7. The ASA upheld a complaint by moneysavingexpert.com and Martin Lewis that the ad misleadingly implied Martin Lewis endorsed the service.[59]

The Moneysavingexpert.com website provides numerous recent examples of ads that use the image of Martin Lewis to misleadingly imply that he endorses scams/products such as binary trading, cryptocurrency investments, energy products and PPI reclaims.[60]

Figure 3.7: Example of unapproved celebrity endorsement

Source: moneysavingexpert.com website

3.1.7 Other harmful ads

Ads may be harmful if they include depictions that might encourage irresponsible behaviour, such as excessive drinking or gambling, unsafe driving, or that glamorise weapons, such as ads for violent computer games or films. In addition, the CAP Code includes specific rules for sensitive category products such as medicines, slimming aids, financial, gambling, lotteries, alcohol, motoring and tobacco. For example, claims about weight loss products must be supported by evidence from rigorous clinical trials. This form of harmful advertising is not specific to online advertising and may occur on other media, such as television, radio and print.

Another example is a Facebook ad run by the alcoholic beverage brand VK in March 2017 which featured an image of a group of people dancing in a nightclub and drinking from bottles of VK. The ASA received a complaint that the image promoted 'unwise drinking styles' and challenged whether the ad was socially responsible. In its ruling the ASA considered that:

> **"the tilted drinking position could be associated with the culture of "downing drinks", particularly in context of the described "squad" group setting."**

[59] https://www.asa.org.uk/rulings/sterling-partnership-ltd-a17-392736.html
[60] https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/

It was concluded that the ad was in breach of CAP Code rules 18.1 and 18.10 (Alcohol). In addition, the ASA challenged that the image had featured people drinking alcohol who appeared to be under 25 years of age and concluded that the ad was in breach of CAP Code rule 18.16 (Alcohol).[61]

3.1.8 Non-identified ads – non-disclosed influencer marketing

Online advertising may be harmful if it is not clearly identified as advertising. Most online display advertising is clearly identified as such, through physical or temporal separation from non-advertising content, and in some cases labelling as an ad or sponsored. However, in influencer marketing the labelling of paid-for posts is generally less clear. The CAP Code requires that:

> 2.1 Marketing communications must be obviously identifiable as such.
>
> 2.3 Marketing communications must not falsely claim or imply that the marketer is acting as a consumer or for purposes outside its trade, business, craft or profession; marketing communications must make clear their commercial intent, if that is not obvious from the context.
>
> 2.4 Marketers and publishers must make clear that advertorials are marketing communications; for example, by heading them "advertisement feature".

In practice, this means that where an influencer is posting about a brand because they have been paid to do so (including payment in kind) and the brand exerts some level of control over the content, the ASA regards the post as an ad which must comply with the requirement that it is obviously identifiable as an ad.[62]

The ASA has issued several recent rulings concerning influencer ad labelling. In August 2019, the ASA upheld a complaint about an Instagram post made by TV personality Olivia Buckland to promote the brand Cocoa Brown[63] (see Figure 3.8).

The visible caption on the post stated "The V-Day prep is well underway and I'm topping up my tan with my fave @cocoabrowntan by @marissacarter 1 HOUR TAN MOUSSE… more". Once the caption was clicked on, additional text stated "Original –it gives me such a natural glow with no streaks and is the perfect accessory for date night with bae [heart eye emoji] Get yours now @superdrug #TeamCB #CocoaBrownTan #ValentinesDay #BrandAmbassador". The ASA considered the post was not obviously identifiable as a marketing communication and as such breached the CAP Code rule 2.1 and 2.4 (recognition of marketing communication). The ASA considered that the term "brand ambassador" was unlikely to convey that Cocoa Brown had both paid for and had a level of control over the content of the post.

[61] https://www.asa.org.uk/rulings/global-brands-ltd-a17-382498.html
[62] ASA (2019). The labelling of influencer advertising.
[63] https://www.asa.org.uk/rulings/cocoa-brown-A19-561238.html

Figure 3.8: Example of a non-identified influencer marketing post

Source: Decision Marketing website article, 7 August 2019[64]

3.1.9 Discriminatory targeting

Targeting focuses advertising on the desired audience, with other audiences being less exposed to this advertising. As such, all targeted advertising inherently discriminates in favour of certain audiences. This may become a problem if the product or offer advertised should be accessible to all, or discrimination is on the basis of protected characteristics. The availability and use of consumer data can allow online advertising to be more effectively targeted than its offline counterparts. This should benefit both parties: advertisers obtain more cost-effective advertising, while consumers receive advertising that is more likely to be of interest to them. Common attributes used in online advertising include demographic indicators such as age, ethnicity, gender, race and sexual orientation, and other parameters such as interests, behavioural information, location and device IDs.

In some circumstances there may be the potential for such targeting to reinforce stereotypes and possibly to discriminate illegally. In the case of products and services where equality of access is important, such as recruitment, any form of targeting can be an issue – depriving certain audiences of access to these products and services. Targeting can also be discriminatory if it is done on the basis of protected characteristics such as race or religion, or proxies for these characteristics, such as postcode, musical taste and travel history.

There is some evidence from previous research studies that discriminatory targeting in online advertising suggests that this can occur at two phases:

1. At the ad targeting phase where advertisers make use of the extensive suite of targeting features offered by ad exchanges and social media platforms, to specify the target audience for their ads; and

[64] https://www.decisionmarketing.co.uk/news/love-island-star-scorched-for-misleading-fake-tan-post. The #ad hashtag shown in the figure is not referred to in the ASA ruling and may have been added afterwards.

2. At the ad delivery phase where the platform delivers ads to specific target audiences according to factors such as advertisers' budget, ad performance and predicted relevance of ads to users.[65]

At the ad targeting phase, techniques such as attribute-based targeting, Personally Identifiable Information (PII)-based audience targeting and look-alike audience targeting could all produce discriminatory outcomes. For example, in a 2018 study researchers identified the potential for Facebook's ad platform to exclude people based on 'ethnic affinity' or to target people interested in or with anti-Semitic viewpoints, and to create large sets of highly biased look-alike audiences using a highly discriminatory source audience.[66] In another example, a randomised controlled experiment run by researchers in 2015 found that Google's ad settings for gender produced outcomes for employment-related ads which differ along gender lines, in particular, browsers set to male gender received more ads for a career coaching service which promoted higher-paying positions than for the female group.[67]

At the ad delivery phase, optimisation algorithms can result in inadvertently biased outcomes even if an advertiser did not take steps to skew their targeting choices. In a study published in 2018, researchers carried out field tests on the delivery of an online advertisement for Science, Technology, Engineering and Math (STEM) jobs and found that fewer women than men were shown the ad on various platforms, such as Facebook, Google, Instagram and Twitter, although the ad itself was explicitly intended to be gender neutral.[68] Another study which was published in 2019 found that skewed ad delivery on Facebook can be influenced by various factors including market and financial optimisation effects, the content of the ad itself, particularly the ad image.[69] The same study also demonstrated significantly skewed delivery for employment and housing ads despite neutral targeting parameters.

The issue of discriminatory targeting has been the subject of several legal challenges in the US in recent years. In October 2019, a class action lawsuit was filed against Facebook alleging that older and female Facebook users have been denied ads about financial services such as bank accounts, loans, insurance and investments.[70] This followed an earlier case in March 2019 in which the US Department of Housing and Urban Development accused Facebook of selling targeted advertising that discriminated on the basis of race, colour, religion, gender, family status, nationality and disability.[71] Facebook has also been involved in other lawsuits involving targeted ad discrimination.[72]

To address some of these concerns of discriminatory targeting Facebook took steps in August 2018 to remove over 5,000 targeting options in order to prevent misuse and to limit the ability for advertisers to exclude

[65] Ali, M et al (2019). *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*. Proceedings of the ACM on Human-Computer Interaction. Available at https://www.ccs.neu.edu/home/amislove/publications/FacebookDelivery-CSCW.pdf

[66] Speicher, T. et al (2018). *Potential for Discrimination in Online Targeted Advertising.* Proceedings of Machine Learning Research 81:1-15, 2018. Available at: http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf [Accessed on 20 March 2020]

[67] Datta A et al. (2015). *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*. Proceedings on Privacy Enhancing Technologies 2015, 92-115. Available at https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf [Accessed on 20 March 2020]

[68] Lambrecht, A and Tucker, CE (2018). *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads*. Available at SSRN: https://ssrn.com/abstract=2852260 [Accessed on 20 March 2020]

[69] Ali, M et al. (2019). *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*. Proceedings of the ACM on Human-Computer Interaction. Article No.: 199. Available at https://www.ccs.neu.edu/home/amislove/publications/FacebookDelivery-CSCW.pdf . [Accessed on 20 March 2020]

[70] PRNewswire (31 October 2019). Facebook Hit with Massive National Civil Rights Class Action by Women and Older People Denied Financial Services Opportunities on Facebook for Years. Available at https://www.outtengolden.com/news/facebook-hit-massive-national-civil-rights-class-action-by-women-and-older-people-denied [Accessed on 20 March 2020]

[71] Reuters (28 March 2019). U.S. charges Facebook with racial discrimination in targeted housing ads. Available at https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8 [Accessed on 20 March 2020]

[72] These include a 2018 class action lawsuit by the American Civil Liberties Union (ACLU) alleging gender discrimination in job advertising on Facebook, and a 2016 class action lawsuit by the Northern District of California against Facebook alleging targeted ad discrimination, by excluding users by ethnic affinity for advertisements on housing credit and job ads.

audiences that relate to attributes such as ethnicity or religion.[73] It also expanded its advertiser education measures requiring all US advertisers to certify compliance with its non-discrimination policy.

For consumers, data-driven online advertising brings the benefits of more relevant ads but also raises concerns relating to privacy and discrimination. A survey of UK adults by Ipsos MORI found that the use of online targeting was seen as broadly acceptable within social media (59%) and advertising (54%).[74] The same study also found that although unfair discrimination against protected characteristics, such as gender, ethnicity and race, was considered undesirable, the extent of concern was lower than other potential areas of harms such as online targeting which exploits vulnerability.

3.1.10 Targeting vulnerable audiences

The availability of targeting tools in online advertising opens up the possibility for online ads to be targeted at audiences who are vulnerable to a particular ad's messaging or content. This form of targeting has the potential to be a problem in the advertising of sensitive category products and services such as slimming aids, medicines and financial services. However, our research found only a limited number of examples of this issue in the paid-for open display and social display advertising segments.

Targeting of vulnerable audiences could be by design, if advertisers choose to use platform targeting tools to select vulnerable audiences or proxies for them. Or it may be inadvertent due to optimisation algorithms learning that vulnerable audiences have a high propensity to click-through, if this is the case. This is related to discriminatory advertising discussed above. Targeting of vulnerable audiences could occur in the open display and social display ad markets, though targeting capabilities differ between providers.

An example is the use of Facebook ads by anti-vaccine groups to target specific audiences with misinformation on vaccine safety (Figure 3.9) by using the platform's tools which allow advertisers to target users classified as being interested in "vaccine controversies". The advert and Facebook page in question were later investigated by the ASA and found to be in breach of the CAP Code rules 3.1 (misleading advertising), 3.7 (substantiation) and 4.2 (harm and offence).[75]

A subsequent research study into vaccine-related advertisements on Facebook found that 54% of anti-vaccine ads over the study period (December 2018 to February 2019) were placed by two organisations.[76] Surveys conducted by the Royal Society for Public Health estimated that two in five (41%) parents are often or sometimes exposed to negative messages about vaccines, and this increased to as many as one in two (50%) among parents with children under five years old.[77] We note that Facebook has been taking steps to tackle the issue of vaccine misinformation, including the removal of targeting options such as "vaccine controversies".[78]

[73] Facebook (21 August 2018). Keeping Advertising Safe and Civil. Available at https://www.facebook.com/business/news/keeping-advertising-safe-and-civil [Accessed 20 March 2020]
[74] Ipsos MORI (February 2020). Public Attitudes Towards Online Targeting. A report for CDEI. Available at https://www.ipsos.com/ipsos-mori/en-uk/public-attitudes-towards-online-targeting
[75] https://www.asa.org.uk/rulings/larry-cook-a18-457503.html
[76] Jamison, AM et al. (2020). Vaccine-related advertising in the Facebook Ad Archive. Vaccine, 38(3), 512-520. Available at https://doi.org/10.1016/j.vaccine.2019.10.066
[77] RSPH (December 2018). Moving the Needle: promoting vaccination uptake across the life course. Available at https://www.rsph.org.uk/uploads/assets/uploaded/3b82db00-a7ef-494c-85451e78ce18a779.pdf
[78] https://about.fb.com/news/2019/03/combatting-vaccine-misinformation/

Figure 3.9: Anti-vaccine Facebook ad

Source: ITV article, 6 November 2018[79]

Another vulnerable audience group is children. Ofcom Children's Media Lives research project[80] – a longitudinal study which follows 18 children, aged 8 to 15, over consecutive years – finds that while most children could identify ads on a range of platforms in the online environment, most younger children believe that advertising was random and not targeted or personalised. There was also a lack of awareness of how the online influencers made money and the nuance of how this could affect influencers' behaviour or the content posted.[81] The research also cited one example of a child watching ads so she could get more virtual 'coins' for gaming while others had seen inappropriate ads for adult content, such as online gambling.

More generally, targeted online advertising could also exacerbate harms across various areas from public health, gambling, mental health issues and general well-being. While rules around the advertising of HFSS products and alcohol are well established in the CAP Code, the impacts of advertising on areas such as vaping (e-cigarettes)[82] and mental health are also emerging areas of concern. For instance, while there are pros and cons associated with vaping,[83] targeted exposure of teenagers to vaping ads has raised concerns that such advertising which is common on social media is drawing in non-smokers.

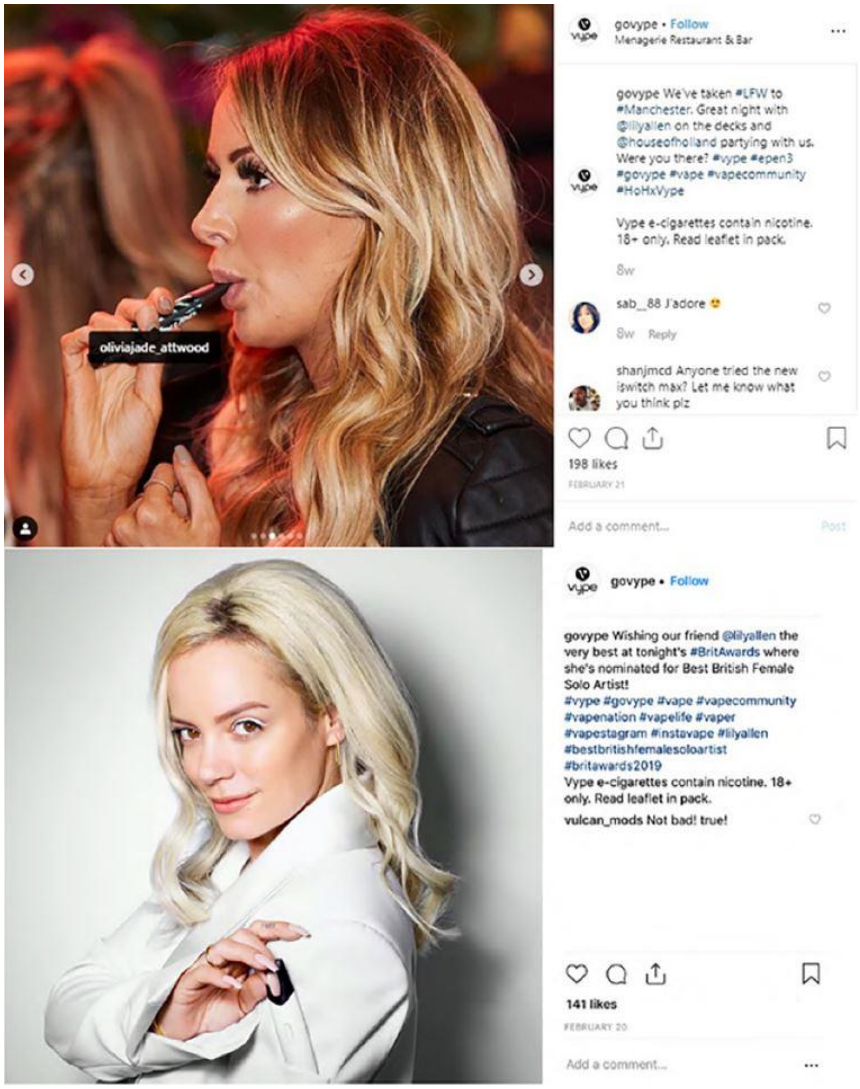
A 2017 survey found that 83% of youths (aged 16 to 19 years) in England have been exposed to some form of vaping product ads, with 40% of exposure coming online through websites and social media, and that more than one-third (38%) of youths found them appealing.[84] In addition, more than a third (36%) of respondents

[79] https://www.itv.com/news/2018-11-06/anti-vaccination-advert-banned/
[80] https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/childrens-media-lives
[81] Revealing Reality (2020). Children's Media Lives – Wave 6. A report for Ofcom. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0021/190524/cml-year-6-findings.pdf
[82] Under the Tobacco and Related Products Regulations 2016, online advertising of e-cigarettes is prohibited.
[83] https://www.bhf.org.uk/informationsupport/heart-matters-magazine/news/e-cigarettes
[84] Cho, YJ et al. (2019). *Youth self-reported exposure to and perceptions of vaping advertisements*: Findings from the 2017 International Tobacco Control Youth Tobacco and Vaping Survey. Preventive Medicine, 126, 105775. Available at https://www.sciencedirect.com/science/article/pii/S0091743519302518?via%3Dihub

perceived that vaping ads target non-smokers. While some of these online ads will be in the form of direct claims on vaping stores' websites, social influencer marketing is also a key avenue of advertising for these vaping products (Figure 3.10).

In relation to the Vype Instagram campaign illustrated in Figure 3.10 the ASA, which prohibits vaping ads on the internet other than provision of factual information about their products on their own websites, found British American Tobacco to have breached CAP Code rule 22.10 and 22.12 (electronic cigarettes).[85] The ads were ordered to be removed and the ASA noted that the promotion of e-cigarettes which were not licensed as medicines should not be conducted from a public Instagram account.

Figure 3.10: Vaping ad campaign on Instagram



Source: PR Week article, 30 April 2019[86]

[85] https://www.asa.org.uk/rulings/british-american-tobacco-uk-ltd-G19-1018310.html
[86] https://www.prweek.com/article/1583293/big-tobacco-confirm-earned-social-media-tactics-ad-authorities-investigate

3.2 What is the scale of inappropriate advertising?

The extent of harmful advertising in the UK is very difficult to quantify due to limited detection and measurement of inappropriate ads in the online advertising ecosystem. However, there are numerous examples of harmful advertising reported in the media and in complaints to the ASA. In addition, the project team saw examples of harmful advertising, mainly malicious advertising, in their day-to-day web browsing and app usage for the duration of the study. Though these examples are not representative of the experiences of consumers more widely, we have included them where relevant.

Importantly, online advertising participants can measure only what they know to be inappropriate, and a significant proportion of harmful advertising may go undetected by the supply chain and unnoticed or unreported by consumers due to the high volume of ads and the nature of targeted online ad campaigns. The data that is available is generally neither consistent nor comparable in terms of definitions, methodologies or segmentations.

We attempted to gather data about the scale of inappropriate advertising in the open display advertising market and the main owned and operated social media platforms. We sought data about three separate measures of inappropriate advertising:

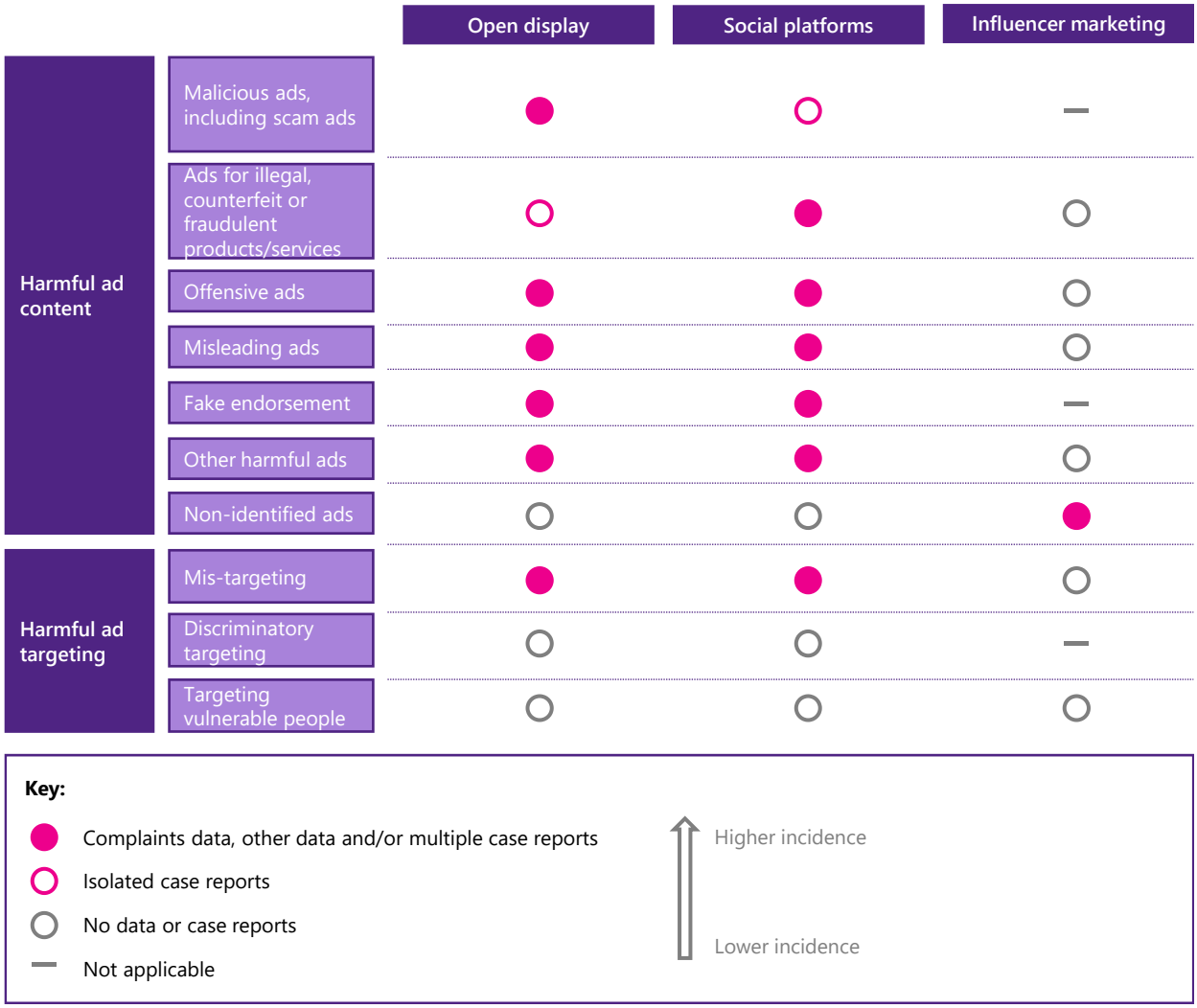
- 'Attempted' – advertiser attempts to run inappropriate ads. Buying platforms (DSPs and owned and operated platforms) generally check ad creative and landing pages for inappropriate content. This data includes ad creatives that are identified as inappropriate and excludes the proportion of creative that is inappropriate and not detected by these checks. Detected inappropriate ads are blocked by the buying platforms and are not served to consumers. The number of impressions that would have been served, had the ad not been blocked, varies by creative. Consequently, the 'attempted' metric does not show the proportion of ad impressions that would have been inappropriate.

- 'Served to users' – consumer exposure to inappropriate ad impressions. These ads evade checks and are served to consumers, and with certain exceptions, are not measured.

- 'Seen and reported' – consumer reports or complaints about inappropriate ad impressions. Consumers may report inappropriate ads to the ASA, publishers and platforms, or other organisations. This data shows the proportion of total paid-for online advertising complaints that are about different categories of inappropriate ad.

Figure 3.11 summarises the relative incidence of consumer-related harms in the online advertising segments considered in this study.

Figure 3.11: Relative incidence of harmful advertising in the UK



The likely scale of inappropriate advertising differs between category of issue:

- Malicious advertising. A cybersecurity expert interviewed for this project believed that about 1% of online open display advertising creatives contain malware and that about one-third of these creatives are not detected and are served to consumers. Cybersecurity vendor Confiant found that about 0.15% of a sample of UK online open display ad impressions were identified as malicious, which would represent hundreds of thousands of ads daily if scaled up to the UK market.[87]

> **"For malware delivery, the advertising ecosystem is the single largest attack vector in the world. The audience is there. It offers perfect targeting. And it [malware] is hard to see because so much of the source code rendering is not from the company that is rendering it [the publisher]. As a delivery vector for ransomware and phishing, web and mobile web [advertising] is bigger than email. It is under appreciated from a cyber security perspective." Chris Olson, CEO, The Media Trust[88]**

- Ads for counterfeit and fraudulent goods and services. The problem of counterfeit goods is recognised by the major online platforms, but there is limited evidence of the scale of paid advertising for retailers

[87] Highly approximate estimate based on the assumption that hundreds of millions of open display ad impressions are served in the UK daily.
[88] Expert interview conducted for this project.

of counterfeit goods relative to organic (non-paid) social posts as a means of promoting these goods. Both Facebook and Google have measures in place for the reporting of content which promotes or sells counterfeit products.[89] They do not disclose how many counterfeit goods ads they stop, though globally Facebook stated that it removed 462,000 pieces of content from Facebook and 359,000 from Instagram in the period from January to June 2019 in response to complaints about counterfeit goods.[90] These pieces of content may be organic social (not paid-for) posts.

- Ads for illegal products. There is limited evidence about online display advertising being used to promote illegal products and services, which appear to be promoted primarily on search, organic social and private messaging platforms. The ASA reports very few complaints about illegal product ads. A law enforcement stakeholder interviewed for this project stated that, in some cases, influencer marketing has been used to encourage criminal activity, such as recruiting money mules.

- Offensive ads. In 2019, 16% of complaints to the ASA about online display advertising (excluding search or social media advertising[91]) related to offensive ads. See Figure 3.12 below.

- Misleading ads. In 2019, 66% of complaints to the ASA about online display advertising (excluding search or social media advertising[92]) related to misleading ads.

- Fake endorsements. In 2019, the ASA received 18 complaints about online display advertising (excluding search or social media advertising[93]) involving fake celebrity endorsements,[94] less than 1% of total complaints about paid-for online advertising. However, there have been many news reports of these ads, indicating that the problem is relatively prevalent.

- Other harmful advertising. In 2019, 11% of complaints to the ASA about online display advertising (excluding search or social media advertising[95]) related to harmful ads, such as harmful depictions that might encourage irresponsible behaviour, ads that glamorise weapons etc.

- Non-identified advertising. In 2019, the ASA received over 1,600 complaints about social influencers, mainly relating to the influencer not disclosing that the content was an ad, paid-for and controlled by the marketer. This volume of complaints is equivalent to more than half of the total number of complaints about open display advertising.

- Misplacement of advertising. ASA avatars research found cases of gambling and HFSS advertising served to child avatars. Avatars simulating children's browsing saw 23 gambling ads 151 times on children's websites – 1.4% of the 10,754 ads they saw on those sites. The avatars methodology does not provide a representative measure of the incidence of exposure to this advertising in the internet population. (See Section 12.1.)

A 2019 survey of internet users on online harms commissioned by Ofcom and the ICO found that among adults concern over scams or frauds was higher (43%) than that of harmful or misleading ads (21%) despite the latter being experienced more frequently – 45% of adults experienced harmful or misleading ads at least weekly

[89] See for example, https://help.instagram.com/499796697033328 (Instagram) and https://support.google.com/merchants/answer/6149993?hl=en-GB (Google)
[90] https://transparency.facebook.com/intellectual-property
[91] Source: ASA. ASA social media complaints data does not distinguish between paid-for advertising and organic posts and is excluded from our analysis.
[92] Source: ASA. ASA social media complaints data does not distinguish between paid-for advertising and organic posts and is excluded from our analysis.
[93] Source: ASA. ASA social media complaints data does not distinguish between paid-for advertising and organic posts and is excluded from our analysis.
[94] These are fake endorsements that link through to ads for products or services which raise serious consumer detriment concerns and potential issues of legality (e.g. products which may not be legally sold).
[95] Source: ASA. ASA social media complaints data does not distinguish between paid-for advertising and organic posts and is excluded from our analysis.

compared to 20% for scams or frauds. The same survey also found that more adults considered scams or frauds to have a more severe impact on them than harmful or misleading advertising (37% compared to 26%).

Figure 3.12: Number of complaints received by the ASA about paid-for online display advertising, 2019

Category	Number of complaints	Proportion of complaints
Offensive ads	517	17.6%
Misleading ads	1,987	67.5%
• of which, fake celebrity endorsement	18	0.6%
Other harmful ads	438	14.9%
Total	2,942	100.0%

Note: This data includes the ASA categories of internet (display), internet (online behavioural advertising), internet video, internet sales promotion and video-on-demand (VOD). The ASA category of social media advertising is excluded because this data does not currently distinguish between paid-for advertising (within the scope of this study) and organic social posts (out of scope of this study). In consequence, the ASA data provides only a partial picture of the number of complaints on advertising within the scope of this study. Complaints about influencer marketing appear in the social media data and are excluded.
Source: ASA

Though online advertising involves a proportion of small-scale advertising campaigns, at its limit dynamic creative campaigns in which individuals see a personalised version of the ad creative. We did not see evidence of a higher rate of harm in these types of campaigns, though data sources generally do not distinguish between large and small-scale campaigns or standard campaigns and dynamic creative.

3.2.1 Measurement and data gathering challenges

The are several reasons that the incidence of inappropriate advertising is difficult to quantify, including:

- **Difficulty of detection.** Malicious advertising is designed to be hidden and can go undetected. Other forms of inappropriate ad content might be too subtly problematic to be easily identified. Supply chain participants measure only the inappropriate ads they can identify – and these are the ads that they are able to block. In consequence, inappropriate ads undetected by the supply chain – the ads that cause consumer harms – are not measured by supply chain participants.

- **Industry participants sharing limited data about inappropriate ad detection.** Supply chain participants who detect and block inappropriate advertising hold data about these inappropriate ads. However, this data is fragmented across numerous participants such as owned and operated platforms and, in the open display market, DSPs, SSPs, publishers and their cybersecurity vendors. Only Google, Facebook and certain cybersecurity vendors publish data, and this is generally very top level or focused on certain issues such as malware. We made data requests to Google and Facebook in an attempt to fill this gap.

- **Limited use of independent panel-based measurement.** It is possible to collect data from a representative panel of UK internet users logging the ad creatives served to these users on certain platforms. These data could be collected, and the creatives sampled and analysed, to provide a definitive view of consumer exposure to inappropriate ad content. However, as we understand it, neither industry participants nor regulators collect panel data for this purpose. The exception is ad-hoc measurement of "in-target" audiences for certain ad campaigns, where the advertiser is interested in understanding whether they have reached the desired audience.

- **Limited consumer reporting of inappropriate ads.** Consumers might not be aware that ads are inappropriate, especially in cases where the ad is subtly problematic, is inappropriately targeted (consumers have limited visibility of how ads are targeted) or is hidden malware. They will not report these ads that go unnoticed. In addition, consumers might not wish to report ads that they know are inappropriate or might not know how to. In consequence, some exposure to inappropriate ads – especially campaigns reaching only small numbers of consumers – might go unreported.

- **Fragmented reporting.** When confronted with an inappropriate ad, consumers could report the ad directly to the publisher or social media platform, use the AdChoices reporting tool (open display only), make a complaint to the ASA or a co-regulatory body, or report a crime or other issue related to the ad to Action Fraud, the Police, Trading Standards or another body. Each organisation will log the report in a different way using different criteria and metrics. In consequence, it is very difficult to develop a joined-up picture of the reporting of inappropriate advertising.

To overcome the lack of publicly available data to monitor inappropriate advertising, there may be a case for the government to consider collecting relevant data from industry participants – or to support original research. There are two main areas where data could be gathered:

- **Consumer reports/complaints.** Social media platforms, publishers and open display advertising intermediaries, as well as regulatory bodies, receive reports or complaints about inappropriate advertising – from consumers and other interested parties, such as brands. The government could ask these organisations to provide regular data about the number of reports they receive, segmented by category of harm and platform, publisher and advertiser. To ensure that this data is consistent, organisations would need to standardise elements of forms used for data collection.

- **Consumer exposure to advertising.** The ASA currently uses avatars to simulate certain groups of consumers and collect data about the ads they would be exposed to on certain services (see Section 12.1). To develop a more robust and representative picture of consumer exposure to advertising would require panel-based measurement. There are challenges to developing a panel covering all relevant devices (desktop, mobile), ad formats (banner, video, native, influencer) and services (open display, social display) and to analyse ads to identify inappropriate ad content. However, this approach might be viable on a limited scale.

3.3 What are the economic and well-being impacts?

The scale of impact of online advertising in relation to the different consumer issues will vary by the nature of the issues and the sectors covered. In general, there is limited quantitative evidence on the scale of the economic and well-being impacts relating the specific issues discussed in Section 3.1. This is not unexpected due to the measurement and data gaps identified above.

3.3.1 Malicious advertising

In terms of economic impacts on consumers, one area where there may be some potentially indicative figures is malicious advertising associated with fraud and scams. In such cases, there is a direct impact on consumers in the form of financial losses. According to research by the Home Office, the estimated total annual cost of fraud against individuals in England and Wales in 2015/2016 was £4.7 billion.[96] The 2017 Annual Fraud Indicator estimated that the total annual cost of fraud against individuals in the UK was £6.8 billion, of which £4.5 billion

[96] Home Office (23 July 2018). The economic and social costs of crime, second edition. Available at https://www.gov.uk/government/publications/the-economic-and-social-costs-of-crime

was due to mass marketing fraud.[97] It is however unclear what proportion of this £4.5 billion is attributable to online display advertising as mass marketing fraud – where fraudsters try to lure victims with false promises of large cash prizes, goods or services in exchange for upfront fees or donations – also covers other activities including unsolicited emails, letters, phone-related fraud. Nonetheless, we note from discussions with relevant stakeholders[98] that fraud cases in which online advertising is used as a means to lure in victims are on the rise.

Although there are no specific figures on the volume of online advertising-related fraud, the Crime Survey for England and Wales (CSEW) estimates that 3.7 million fraud incidents in the year ending December 2019, and another 900,000 computer misuse offences experienced by the adult population over the same period.[99] In terms of the proportion of cyber-related fraud incidents, the CSEW estimates this to be 54%[100] while Action Fraud reports 86%.[101,102]

There is evidence that fraudsters are buying online advertising and the share of advertising estimated to be malicious (0.15%) suggests that fraudsters are spending at least single figure millions of pounds annually, and they would expect a high return on this investment, suggesting that consumer losses are at least in the tens of millions.

In addition to the economic impacts, victims of malicious advertising also experience negative emotional and well-being impacts. According to the CSEW, over three quarters (76%) of victims of fraud and computer misuse offences were emotionally affected with 31% of victims being significantly affected, i.e. respondents who were affected 'quite a lot' or 'very much'.[103]

In addition to financial loss by consumers, malicious advertising also contributes to ad fraud through botnets created by infected computers which are then used to create invalid traffic. We discuss ad fraud in more detail in Section 4.1.

3.3.2 Counterfeit goods

Another area where there is clear and direct economic impact is ads for counterfeit goods. The scale of trade in counterfeit goods is significant. The OECD estimates that imports of counterfeit and pirated goods to the UK accounted for as much as £13.6 billion in 2016 – equivalent to 3% of UK imports of genuine goods – and these cover a wide range of products such as electronics, clothing, footwear and pharmaceuticals.[104] For consumers, counterfeit goods pose risks to health, safety and privacy, and could also lead to lower consumer satisfaction, particularly when low-quality fake goods are purchased unknowingly. The OECD estimated that consumer detriment due to deception on primary markets, namely in terms of the premium unjustly paid by consumers in the belief that they are buying a genuine product, was almost £4.8 billion in 2016.[105]

[97] Crowe UK, Experian and the Centre for Counter Fraud Studies (November 2017). University of Portsmouth. Annual Fraud Indicator 2017: Identifying the cost of fraud to the UK economy. Available at https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Annual-Fraud-Indicator-report-2017

[98] Such as the National Fraud Intelligence Bureau and technology vendors.

[99] Office of National Statistics (23 April 2020). Crime in England and Wales: year ending December 2019. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2019

[100] Office of National Statistics (19 March 2020). Nature of crime: fraud and computer misuse. Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

[101] Action Fraud (2019). National Fraud Profile. https://data.actionfraud.police.uk/cms/wp-content/uploads/2019/06/National_Fraud.pdf

[102] The differences are due to the methodologies used by CSEW and Action Fraud. The CSEW uses routing questions about the crime to understand whether it was cyber enabled, whereas the Action Fraud's figure is based upon the type of fraud as categorised by the National Fraud Intelligence Bureau (NFIB) codes that the victim reported at the time of the crime.

[103] Office of National Statistics (19 March 2020). Nature of crime: fraud and computer misuse.

[104] OECD (November 2019). Trade in Counterfeit Products and the UK Economy. Available at https://www.oecd.org/gov/risk/trade-in-counterfeit-products-and-uk-economy-report-update-2019.pdf

[105] It should be noted that the extent to which online advertising plays a role in causing such harm will vary by the type of goods. For example, online advertising of counterfeit goods is likely to be much more prevalent in the category of clothing, footwear and leather, than that of machinery, industrial equipment and computers.

Online advertising is likely to have a role in the marketing of counterfeit goods and thus contributes directly to the economic impact, although there is limited evidence on the proportion of counterfeit sales attributable to paid-for online advertising. Moreover, online advertising is not the only factor that explains the consumption of counterfeit goods. Firstly, there are also other marketing means for such goods (e.g. offline, search and organic social media). Secondly, this is a problem that is likely to persist independent of advertising as peddlers of such goods have a financial incentive to sell them to unknowing consumers. Thus, while the OECD figures suggest that the scale of the problem of counterfeit goods is substantial, the impact that can be directly attributed to online advertising is likely to be considerably smaller.

3.3.3 Other areas

In the other areas discussed in Section 3.1, quantitative evidence on socio-economic impacts tends to be broader in scope, taking an economy-wide perspective in specific areas such as alcohol,[106] drugs,[107] gambling[108] or smoking.[109] In many of these areas, the linkages between advertising and such activities have been acknowledged and subject to considerable amount of research, but there are often multiple interrelated causes underlying the economic and social harms in these areas. Evidence on the scale of harm in monetary terms which is directly associated with online advertising is scarce.

One emerging area of concern is mental health issues arising from the portrayal of body image and gender stereotypes in the media including advertising. This has been the subject of a number of recent studies, for example, a survey commissioned by the Mental Health Foundation[110] found that:

- Just over one in five adults (21%) said images used in advertising had caused them to worry about their body image; and
- Just over one in five adults (22%) and 40% of teenagers said images on social media caused them to worry about their body image.[111]

The exposure to unrealistic 'ideal' and unrealistic bodies through different media forms – film, television, magazines, advertising and social media – has been linked to anxiety, depression and unhealthy eating behaviours.[112,113] A study commissioned by Beat, an eating disorder charity in the UK, estimated that the economic cost arising from eating disorders could be up to £16.8 billion per year.[114]

The ASA has emphasised that ads should be socially responsible and has clamped down on ads which are judged to have an adverse impact on mental health and on society in general. For example, a Ladbrokes online

[106] Institute of Alcohol Studies (2016). The economic impacts of alcohol. Available at http://www.ias.org.uk/uploads/pdf/Factsheets/FS%20economic%20impacts%20042016%20webres.pdf
[107] Singleton, N et al (2006). Measuring different aspects of problem drug use: methodological developments. Home Office Online Report 16/06. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116642/hoor1606.pdf
[108] Institute for Public Policy Research. Cards on the Table: The cost to government associated with people who are problem gamblers, December 2016. Available at https://www.ippr.org/files/publications/pdf/Cards-on-the-table_Dec16.pdf
[109] Epku, VU and Brown AK (2015). The economic impact of smoking and of reducing smoking prevalence: review of evidence. Tobacco Use Insights, 8: 1–35. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4502793/
[110] Mental Health Foundation (May 2019). Body Image: How we think and feel about our bodies. Research Report. Available at https://www.mentalhealth.org.uk/publications/body-image-report
[111] It should be noted that images on social media will include paid-for online advertising and organic social media posts.
[112] Be Real Campaign (January 2017). Somebody Like Me: A report investigating the impact of body image anxiety on young people in the UK. Available at https://www.berealcampaign.co.uk/wp-content/uploads/2018/02/Somebody_like_me-v1.0.pdf
[113] Royal Society for Public Health (May 2017). StatusOfMind: Social media and young people's mental health and wellbeing. Available at https://www.rsph.org.uk/uploads/assets/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf
[114] PwC (February 2015). The costs of eating disorders: social, health and economic impacts. Available at https://www.beateatingdisorders.org.uk/uploads/documents/2017/10/the-costs-of-eating-disorders-final-original.pdf

ad was found to be in breach of the CAP Code for suggesting that gambling could provide an escape from personal problems such as depression or that it can be a solution to financial concerns.[115]

It should be noted that online advertising is just one of a number of contributing factors, and we have not identified any research or study that has assessed the scale of harm caused by online advertising in this area. A survey commissioned by the ASA on gender stereotypes in advertising found a negative impact on attitudes and behaviour due to nudity and emphasised sexualisation in ads, but respondents also believed that social media content was often more problematic than advertising.[116]

Moreover, the impact of advertising in this area is not unambiguously negative and advertisers can play a role in ensuring that ads reflect diversity and reality. For example, major companies such as Dove and Unilever have signed up to the 'Be Real Body Image Pledge' by the Be Real Campaign by committing to reflect diversity and reality in their messages and advertising, and to promote health and well-being.[117]

3.4 Participants and causal chain

Inappropriate advertising may be placed by a range of advertisers, from organised cyber criminals to legitimate brands and small businesses. Figure 3.13 shows the types of advertisers generally responsible for different categories of inappropriate advertising.

Figure 3.13: Advertisers responsible for inappropriate advertising

Note: categories are not mutually exclusive.

[115] https://www.asa.org.uk/rulings/ladbrokes-betting---gaming-ltd-a17-388937.html
[116] ASA (July 2017). Depictions, perceptions and harm: a report on gender stereotypes in advertising. Available at https://www.asa.org.uk/resource/depictions-perceptions-and-harm.html
[117] Be Real Body Image Pledge. Available at https://www.berealcampaign.co.uk/resources/be-real-body-image-pledge

Consumers may be exposed to harmful advertising due to advertisers acting irresponsibly, limited or ineffective controls within the advertising supply chain, and difficulty with timely reporting and stopping of harmful ad campaigns. Figure 3.14 sets out a generalised chain of events and contributing factors.

Figure 3.14: Factors enabling consumer exposure to harmful advertising

Chain of events:	1. An advertiser attempts to run an inappropriate ad campaign	2. Supply chain participants enable the ad to be served	3. Few if any consumers report the ad	4. The supply chain is slow to respond and stop the ad
Contributory factors:	• Criminal actors are able to operate scams, hacking and other malicious enterprises and buy advertising to support this activity • Legitimate advertisers might not be aware of rules and best practices or they deliberately breach these standards	• Large volumes of ads are run every day • Inappropriate advertising is difficult to detect using automated methods • Defences against inappropriate ads are uneven across vendors • Supply chain participants have limited incentive to stop inappropriate ads • In open display, the supply chain is complex and opaque, such that criminal actors can hide	• Consumers might not be able to identify ads or targeting as being inappropriate • Consumers might not see the benefit of reporting bad ads • Consumers might not understand how to report inappropriate ads • Reporting mechanisms on some platforms are limited or not user friendly	• In open display, it is technically complex to trace and stop ads across different vendors

The nature of these factors and the participants involved differ between the types of harmful advertising described above. The following sections explain the drivers of harmful advertising in each case.

At stage 2 in the chain of events, above, the supply chain participants involved differ between market segments. In the open display advertising market, there is a complex ecosystem of participants that generate ad inventory and facilitate the programmatic trading of this inventory – as illustrated on Figure 3.15. In the social display market, owned and operated platforms such as Facebook, Google-YouTube, Twitter and Snapchat are responsible for the end-to-end supply chain – equivalent to publisher, ad server, SSP and DSP combined in the open display market.

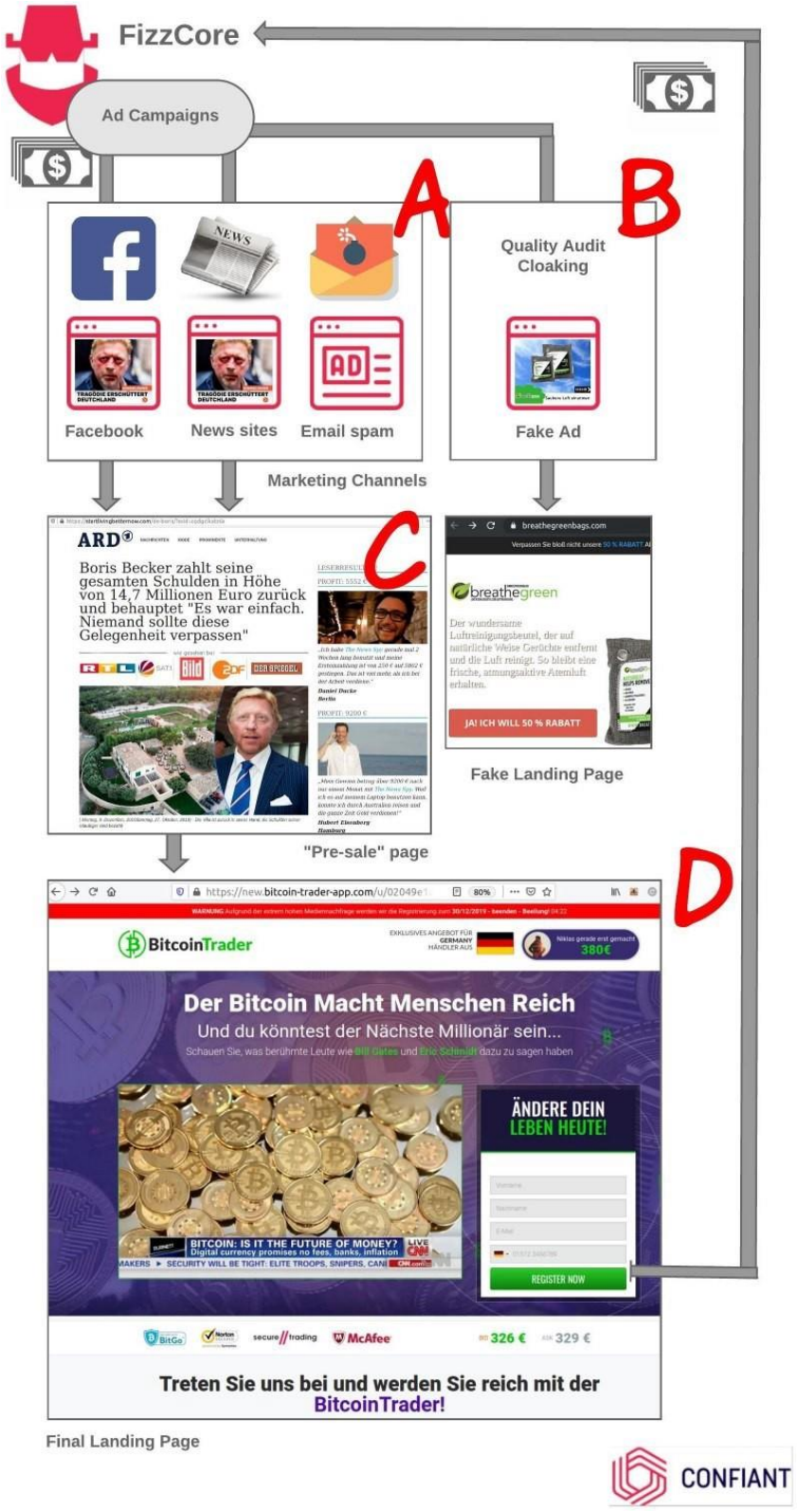
Figure 3.15: Programmatic online advertising supply chain – simplified[118]

[118] Spark Ninety (January 2020), Transparency in programmatic online display advertising markets: Presentation to the 6th meeting of the expert group for the European Commission Observatory on the Online Platform Economy.

3.4.1 Malicious advertising

This section relates to malicious advertising in the open display advertising market. Malicious advertising is generally placed by organised cyber criminals to draw consumers into scams, hack their systems, or hijack their computing resources for nefarious purposes such as botnets or cryptomining. In many cases, paid-for online display advertising is just one element of a wider criminal enterprise. Figure 3.16 illustrates the role of malicious advertising in an example of a scam – in this case in Germany – that follows a similar model to the scam illustrated in Figure 3.3, above.

Figure 3.16: Structure of a bitcoin scam involving malicious advertising



In this case: (A) paid-for celebrity clickbait ads are placed on websites, (B) a placeholder ad and landing page are used to pass quality audits, (C) the ad clicks through to a fake news site promoting the investment, and (d) the fake news site clicks through to the actual scam.

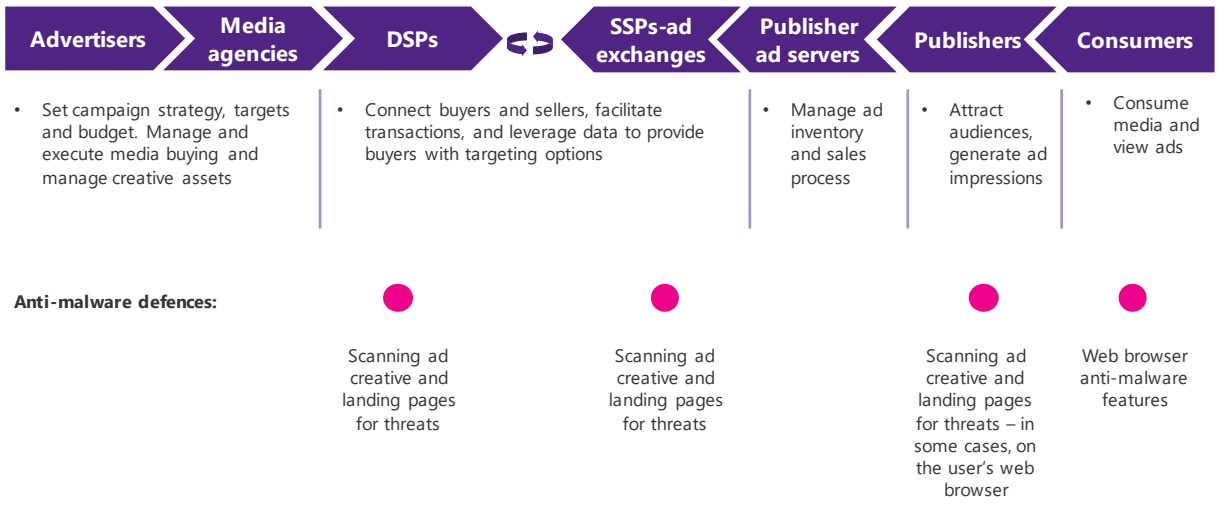
A cybersecurity firm interviewed for this study estimated that there are about 10 to 15 major cyber-crime groups responsible for malicious advertising attacks; another expert believed that there are about 1,000 attacks ongoing at any one time. These cyber-criminal groups often launch attacks internationally from locations around the world. Industry experts believe that perpetrators of malvertising are especially prevalent in Eastern Europe and the Asia Pacific region. Each of the main groups is recognisable by its methods, such as the use of particular types of scam ads, but their true identity is unknown.

In order to run a malicious ad campaign, cyber criminals need to buy ad inventory. In the open display advertising market, demand-side platforms (DSPs) are the main point of access to this ad inventory. In one case in 2017, a cyber-criminal group set up 28 fake advertising agencies in order to buy programmatic advertising on DSPs.[119] Some DSPs' vetting of new customers does not appear to prevent criminal actors setting up accounts. A cybersecurity firm interviewed for this study noted a lack of "know your customer" procedures, such as checks on the source of funds used to buy online advertising.

In 2018, cyber-criminals set up their own fake DSP, enabling them to buy advertising inventory directly on programmatic ad exchanges.[120] In this case, the fake DSP Amobi spoofed the genuine DSP Amobee. This approach enabled the cyber-criminals to bypass legitimate DSPs – and any checks DSPs make on new accounts and on ad creative (see below).

Once cyber-criminals have plugged into the programmatic ecosystem and are enabled to buy advertising, they need to ensure that their malicious ad creative passes quality controls put in place by supply chain participants – as illustrated in Figure 3.17. DSPs, SSPs and some publishers perform automated scans and, in some cases, human review of ad creative and landing pages. In addition, some publishers use dedicated blockers or cybersecurity services such as Confiant to protect against malicious advertising that evades DSP and SSP defences.

Figure 3.17: Anti-malware quality controls in the programmatic open display advertising market



It is challenging to deliver strong, up-to-date anti-malware scanning and browser blocking.

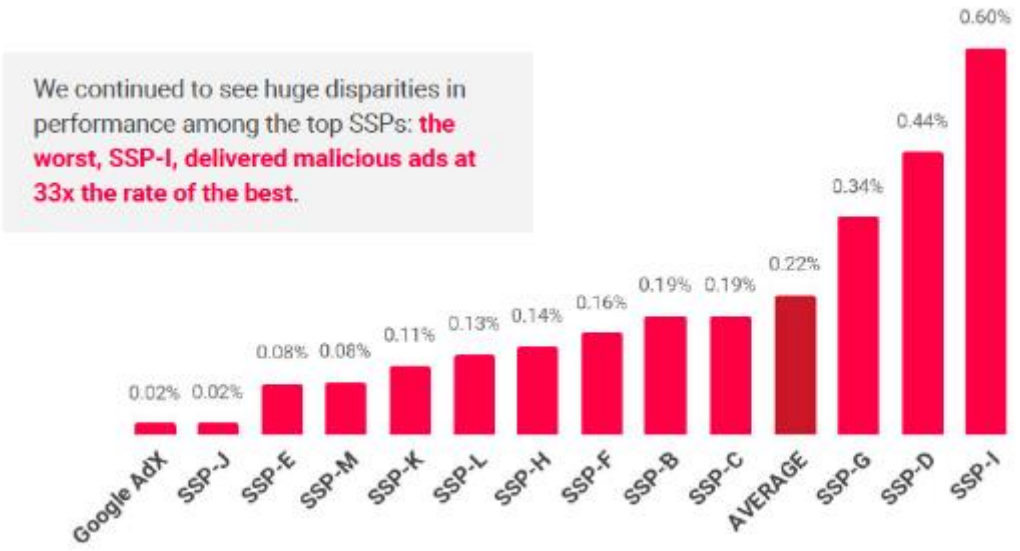
> ***"Malvertising is very difficult to detect. Blockers don't block things they have not detected. Knowing what is bad quickly is really hard … And blockers act as a giant billboard saying I'm here to stop you"*** **Chris Olson, CEO, The Media Trust[121]**

[119] https://blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85
[120] https://www.adexchanger.com/online-advertising/fraudsters-are-masquerading-as-real-dsps/
[121] Interview conducted for this project.

As we understand it, cyber-criminals are constantly developing new techniques to overcome DSP and SSP defences. Their strategies range from highly sophisticated attempts to hide malicious code, to brute-force bombardment of vendors with large numbers of creative variants. The Media Trust identified an attack that it named GhostCat in which a malicious URL was hidden using concatenation and encoding to avoid detection by publisher blockers. The attack also probed whether its own malicious Javascript had been added to blocking scripts – possibly enabling the attackers to monitor security defences.[122]

Cyber-criminals need only overcome the defences of one DSP and SSP in order to establish a supply path and serve malicious advertising. It is likely that smaller SSPs have the weakest defences due to a lack of funding, resources and data relative to major players. Research from cybersecurity vendor Confiant shows that in the USA the worst performing SSP has a 33-times higher rate of malicious ad impressions than Google AdX, the best performing SSP.[123] However, this data shows only the attacks that were detected by Confiant. It is likely that some attacks went undetected – including on the SSPs that are shown to be strongly performing on this chart.

Figure 3.18: Rates of malicious impressions by SSP, USA, Q4 2019[124]



Source: Confiant, Demand Quality Report, Q4 2019

In many cases, consumers are not aware that they have been affected by malicious advertising. The ad could appear innocuous and the malware it propagates may operate unnoticed. In cases where malware leads to hacking and cyber criminals using stolen credit card details, the consumer might not attribute this problem to malicious advertising. Some industry participants believe that it is difficult for law enforcement authorities to act without attribution of a victim to a malicious advertising attack.

Cyber criminals generally buy advertising inventory at a large scale in order to maximise the reach of their campaign before consumers and/or the supply chain notice the attack and stop it. Consumer reporting of malicious advertising when they notice it might be impeded by a lack of clear guidance over how to report malicious ads (see Section 3.4.6 below). Once an ad has been reported, the supply chain response could be slow due to:

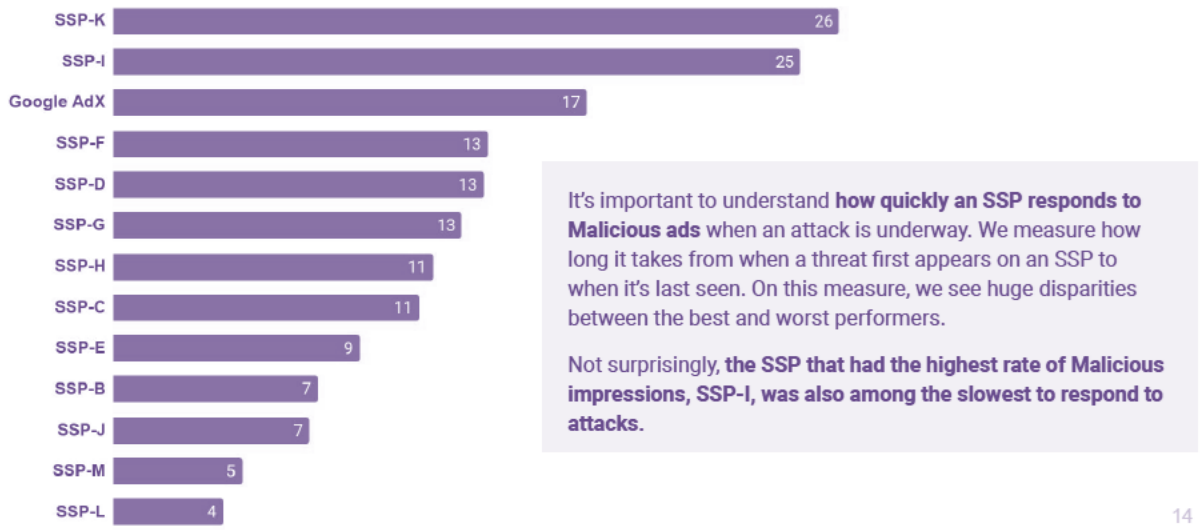
[122] The Media Trust, GhostCat-3PC, Malware targets well-known publishers and slips through their blockers.
[123] Confiant (2019), *Demand Quality Report*, Q4 2019.
[124] SSPs A to L include Google AdX, Rubicon Project, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, EMX, Sonobi, TripleLift, District M, 33Across, and Sovrn.

- **Complexity of the supply chain.** In the case that a consumer reports a malicious ad to a publisher, the publisher will need to investigate and report the ad to its SSP partners who in turn will need to identify and block the DSP seats responsible and liaise with DSPs to block the malicious demand at source.

- **The lack of a universal creative ID.** Each online advertising creative is given a different ID – a unique identification code – on each platform. A malicious ad discovered on one platform may be difficult to find and take down on other platforms. When asked for the one thing the industry should support to improve ad quality, the second-ranking response mentioned by 22% of respondents was "Universal creative IDs to make tracking bad ads easier".[125]

- **Slow responses from supply chain participants.** Some SSPs and DSPs might be slow to act on reports of malicious advertising. Research from cybersecurity vendor Confiant shows that malicious advertising campaigns ran for an average of 4 days on the best performing SSP in the USA and 26 days on the worst performing SSP.[126] However, this data is complicated by differences in the type of attacks that each SSP experiences – the times for SSPs that successfully block most attacks are measured on the basis of the small number of more challenging attacks that get through.

Figure 3.19: Average malware attack response time by SSP in days, USA, Q4 2019[127]



Source: Confiant, Demand Quality Report, Q4 2019

3.4.2 Ads for illegal, counterfeit or fraudulent products and services

Participants in the online advertising supply chain generally have policies in place that prohibit advertising of illegal products and services. For example, Xandr prohibits ad content featuring the sale of weapons and illegal drugs, and content in violation of applicable law, regulation or court order.[128] Facebook prohibits ad content such as illegal products or services, weapons and infringement of third-party intellectual property.[129]

[125] Ad Lightning (2020). *The 2020 State of Ad Quality Report*.
[126] Confiant, *Demand Quality Report*, Q4 2019
[127] SSPs A to L include Google AdX, Rubicon Project, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, EMX, Sonobi, TripleLift, District M, 33Across, and Sovrn.
[128] Xandr, *Policies for Buying*, Accessed 5 March 2020. https://wiki.xandr.com/display/policies/Policies+for+Buying
[129] Facebook, *Advertising Policies*, Accessed 5 March 2020. https://www.facebook.com/policies/ads/

Owned and operated online advertising platforms and open display advertising vendors (DSPs, SSPs, and some publishers) generally perform checks on advertising creative. However, it appears that these checks do not stop all ads for illegal and counterfeit products.

Consumers reporting ads for illegal or counterfeit products may experience the same challenges described in Section 3.4.1. In the open display advertising market, they might not know where or how to report advertising or they may report the retailer of counterfeit goods to trading standards or the police, and not report the advertising.

In the case of counterfeit goods ads, brands can also play a role in identifying problems. Facebook helps brands to identify and report IP infringement. The Facebook Commerce and Ads IP Tool enables registered trademark owners to search ad text and titles across Facebook and Instagram, review ad content for intellectual property infringement and report content to Facebook. Facebook also provides a Counterfeit Report Form[130]. Snapchat enable brands to report content infringing trademarks,[131,132] but they do not provide tools for brands to search paid-for ads for infringement. YouTube provides a Counterfeit Complaint form.[133]

3.4.3 Other harmful ad content

Advertisers for other inappropriate ad content, such as misleading and offensive ads, include a wide range of organisations. In the period 1 January 2020 to 4 March 2020, the ASA upheld complaints about paid-for internet advertising against organisations including online retailers The Hut.com[134] and Prettylittlething.com,[135] vaping retailer Nicoventures Retail[136] and an Estonian seller of face masks, Novads OU.[137]

There is limited information about why these organisations place inappropriate advertising. In the case of larger-scale legitimate advertisers, the reason may be a lack of awareness or education about the detail of the CAP Code, and/or a lack of attention to compliance. Smaller-scale advertisers might not be aware of the code or intentionally break the rules. Some overseas advertisers such as Novads OU might deliberately disregard the code, given the limited risk to them of breaking these rules.

As noted in Section 3.4.2, supply chain participants generally have policies prohibiting certain advertising. These policies mirror elements of the CAP Code. The supply chain conducts quality checks on advertising creative, as described in Section 3.4.2. The way that these quality checks work is not documented, given security considerations. In some cases, these checks involve the use of automated scans that may use AI to learn to identify inappropriate content and landing pages. Human review or escalation is also involved in some cases. However, it is likely to be challenging to accurately review advertising creative for compliance against the full breadth of the CAP Code.

As noted in sections and 3.4.1 and 3.4.2, consumers might not identify inappropriate advertising as such and might not report advertising that they do identify as inappropriate.

[130] https://www.facebook.com/help/contact/counterfeitform
[131] https://help.instagram.com/222826637847963?helpref=page_content
[132] https://support.snapchat.com/en-US/a/infringement-trademark-general
[133] https://www.youtube.com/reportingtool/counterfeit?rd=1
[134] https://www.asa.org.uk/rulings/the-hut-com-ltd-cas-564984-g8j2w5.html
[135] https://www.asa.org.uk/rulings/prettylittlething-com-ltd-cas-583039-y6l1x6.html
[136] https://www.asa.org.uk/rulings/nicoventures-retail-uk-ltd-A19-1027961.html
[137] https://www.asa.org.uk/rulings/novads-ou-cas-599611-h1h2q1.html

3.4.4 Non-identified advertising

Influencer marketing is a relatively new form of marketing and regulatory compliance is this area is less well developed than in online display advertising. The lack of clear identification of some paid-for social influencer posts as advertising may be due various factors, including:

- Influencers are individuals and may have less skills and capacity to deal with compliance issues than publishers and platforms in the display advertising market.
- Influencers might not be aware of relevant rules or understand how to apply them. The ASA and CMA have published a simple guide to labelling influencer marketing,[138] but some influencers might not be aware of this guide.
- Platform tools for labelling paid-for posts might not be consistent with regulatory guidance. On Instagram, when influencers tag a business partner (sponsor) people will see "Paid partnership with…" above the post.[139] However, the ASA and CMA advise using words such as "Ad", "Advert", "Advertising", and state that "Other labels are riskier, and although it will always depend on the wider content and context, we usually recommend staying away from; Supported by/Funded by, In association with, Thanks to [brand] for making this possible, Just @ [mentioning the brand}, Gifted and Sponsorship/Sponsored".[140] The risk referred to is likely to be the danger of the label not being noticed or understood.

3.4.5 Inappropriate targeting

With the exception of mis-targeting of alcohol, gambling and HFSS advertising at children,[141] there is very limited generally agreed codification of what constitutes inappropriate targeting. The ethics of targeting are relatively undeveloped. The Centre for Data Ethics and Innovation (CDEI) conducted research into targeting practices and recommended that the government introduces regulatory oversight of organisations' use of online targeting systems through the proposed online harms regulator.[142] The CDEI proposes that the regulator develop a code of practice focusing on targeting processes and covering risk management and transparency. However, at present, there are limited measures in place to prevent inappropriate targeting, over and above the protections afforded through GDPR compliance.

Certain owned and operated platforms such as Facebook offer very powerful targeting tools. And in the open display market, advertisers can target at a granular level based on first-, second- and third-party data. Given this situation, it is possible for advertisers to set up campaigns that are discriminatory or target vulnerable audiences. In the case of legitimate advertisers, this targeting might be inadvertent or not fully thought through. However, cyber criminals appear to be unrestrained in targeting inappropriately. Cybersecurity experts interviewed for this study believe that cyber criminals engaged in malware attacks use targeting in the open display advertising ecosystem to reach vulnerable devices and software, and vulnerable and/or high value users.

The ability of supply chain participants to identify and control inappropriate targeting is limited. Facebook has policies that prohibit use of targeting options to 'discriminate against, harass, provoke or disparage users, or to engage in predatory advertising practices'.[143] Facebook requires all advertising users to certify compliance with

[138] https://www.asa.org.uk/uploads/assets/9cc1fb3f-1288-405d-af3468ff18277299/INFLUENCERGuidanceupdatev6HR.pdf
[139] https://help.instagram.com/116947042301556
[140] https://www.asa.org.uk/uploads/assets/9cc1fb3f-1288-405d-af3468ff18277299/INFLUENCERGuidanceupdatev6HR.pdf
[141] These are addressed in the ASA's CAP Code. In addition we note that the Gambling Commission has proposed industry measures, to be in place by July 2020, aimed at reducing the amount of online advertising seen by children, young people and vulnerable adults. https://www.gamblingcommission.gov.uk/news-action-and-statistics/News/gambling-commission-and-industry-collaboration-makes-progress-on-safer-gambling
[142] CDEI (4 February 2020). Review of online targeting: Final report and recommendations.
[143] https://en-gb.facebook.com/policies/ads/

its non-discrimination policy, and as mentioned in Section 3.1.9 above, it has removed a number of targeting options which could be used in a discriminatory manner and expanded its advertiser education policy. Google has policies around data collection and use in personalised advertising, but it does not explicitly restrict practices such as discriminatory targeting.

Consumers have limited ability to understand how and why an ad was targeted to them. In the open display market, AdChoices enables consumers to see that an ad was targeted based on browsing history, for example, but not which specific characteristics it was targeted on. On Facebook, users are able to access more information. Consumers who click on the '…' symbol at the top right-hand corner of an ad, then click 'Why am I seeing this ad?' are provided with information about how the ad is targeted, such as the specific interest, demographics and location. In the open display market, consumers are unlikely to have sufficient information about how a specific ad has been targeted to them to know whether or not this targeting is inappropriate.

3.4.6 Reporting mechanisms

At present there are a number of ways that a consumer can report or make a complaint about an ad, including

1. clicking on a reporting mechanism built-in to the ad unit (such as on the AdChoices logo – see Section 7.2.3),

2. reporting the ad to the media owner/platform using a dedicated form or a general form or email; for example, Google[144] and Instagram,[145]

3. reporting the ad to the ASA,[146]

4. reporting the ad (or associated landing page or scam) to another body with remit of specific sector or issues, such as the FCA (financial scams[147]), ICO (privacy, data-related issues[148]), Action Fraud[149] or Citizens Advice.[150]

The ASA has memoranda of understanding with various organisations on sharing relevant information and handling complaint cases.[151] However we observe some potential issues with the current system, namely:

- No 'one-stop shop' solution – the presence of different reporting mechanisms and steps involved is likely to be confusing to consumers.

- A lack of clarity in how complaints are dealt with could deter consumers from raising complaints. For example, a consumer reporting an ad on Google receives a message "Thanks. Feedback improves Google Ads" and a similar message is provided upon reporting an ad on Instagram "Thanks for letting us know. Your feedback improves the quality of ads on Instagram."

- Potential overlaps in some cases (e.g. scam reporting can be done through several bodies) although the NFIB do coordinate across these different agencies.

In many cases, the incentives to report bad advertising are likely to be low and consumers may not bother especially if the level of harm or financial loss at an individual level is low, and there is no assurance that the

[144] https://support.google.com/google-ads/troubleshooter/4578507?rd=1
[145] https://help.instagram.com/1415228085373580
[146] https://www.asa.org.uk/make-a-complaint.html
[147] https://www.fca.org.uk/consumers/report-scam-us
[148] https://ico.org.uk/make-a-complaint/
[149] https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime
[150] https://www.citizensadvice.org.uk/scamsaction/
[151] These include organisations such as the CMA, ICO, DEFRA, Financial Conduct Authority and Gambling Commission,

complaint will be dealt with in an appropriate way. We understand from some stakeholders that there may be a significant amount of low-level online scam activity that goes unreported. Another factor could be a tendency of some scam victims to be too embarrassed to admit they were scammed.[152]

Aside from scams/frauds where the harm is direct and immediate suffered in most cases, other categories of harms are either indirect or non-financial and potentially subjective (offensive ads, misleading) or tend to manifest themselves in the long run (impacts on physical or mental health, social effects). For such categories there may be fewer incentives for consumers to report instances of inappropriate online advertising or targeting.

[152] For example: https://www.bbc.co.uk/news/education-44629881

4 Advertiser issues

4.1 Advertising fraud

Summary

Nature:	Wide range of sophisticated frauds that counterfeit ad inventory or ad measurement metrics.
Scale:	Estimated £20 million to £100 million in the UK in 2019, but potentially much higher – very limited data.
Market:	Mainly programmatic online display advertising. Social media advertising experiences less fraud.
Victims:	Advertisers and publishers.
Impact:	Direct financial losses, indirect costs such as decreased ad spend.
Perpetrators:	Mainly sophisticated cyber-criminal operations at a global scale.
Causes:	Market complexity, lack of adequate checks on vendors of ad inventory.

4.1.1 What is online advertising fraud?

Online advertising is an intangible product. Trading of online advertising is done on the basis of information about the audience for and context of an ad impression, and in some cases desired actions such as click-throughs or sales. In the programmatic ad market, this information about an impression may pass through several vendors, with limited verification along the way. There is substantial scope for falsifying this information in order to create counterfeit online advertising. Ad fraud generally involves one or more of the following components:

1. Fake traffic. At the extreme, fraudsters create entirely fake online advertising. They use botnets to mimic the actions of consumers viewing online advertising and generate vast volumes of ad impressions that are never seen by humans. This practice is generally referred to as invalid traffic (IVT) fraud. Or fraudsters may insert code into ad units to serve multiple ads that are hidden to the user.

2. Fake audience data. Fraudsters may falsify audience data to make advertising appear more valuable. In the case of geo-fraud, fraudsters buy ad impressions in low-price markets such as Afghanistan then tamper with geo data and resell these impressions as UK or US audiences, at a far higher price. In the case of bot traffic (above), fraudsters may instruct bots to browse certain websites to generate a data trail indicating that the bots are high-value users, such as people in the market for top-of-the-range cars.

3. Fake context. To make fake ad impressions appear attractive to advertisers, fraudsters may attempt to pass these impressions off as originating from a quality content site. This practice is known as domain spoofing. Fraud may also involve arbitrage of genuine ad impressions. Fraudsters may buy low-price ad

formats, such as commoditised inventory on mobile apps, and pass these ad impressions off as high-value inventory such as connected TV advertising.

4. Fake actions. In cases where advertisers pay for actions, such as click-throughs, fraudsters may fake these clicks using malicious bots, click farms or ad-fraud schemes and take a share of commission fees from complicit websites or ad networks. Providers of mobile apps may pay for advertising on the basis of app installs, and attribution of these installs may be faked by fraudsters by generating fake click throughs.

Overall, there are multitude of different specific types of ad fraud which may include one or more of these elements. Examples of specific cases and types of fraud are provided in Appendix C.

4.1.2 What part of the online advertising market does fraud affect?

Our assessment is that the market most susceptible to fraud is open display advertising, particularly advertising inventory sold on programmatic open exchanges. The complexity of the programmatic supply chain provides opportunities for fraudsters to interface with genuine vendors and to monetise counterfeit advertising inventory, or to perpetrate other types of fraud.

Fraudsters are generally attracted to categories of online advertising that offer the highest rewards, in terms of price, and the weakest security measures. Cybersecurity vendor data shows that fraud is most prevalent on mobile applications and connected TV, while desktop display and video are relatively safer. The World Federation of Advertisers Digital Media Benchmark shows reported fraud rates of 2.0% in display, 1.8% in mobile in-app, and 1.4% in video in Western Europe.[153]

It is likely that owned and operated advertising platforms such as Facebook, Instagram, YouTube and Snapchat are generally safer environments, given that they control the end-to-end supply chain. Third parties such as fraudsters do not participate in this chain. However, in the case of influencer marketing, there is the potential for influencers to attract fake followers, such that the follower metrics they trade against are false. On Instagram, researchers reported a fake engagement rate on certain accounts with the least authentic audiences increase from 1% in September 2019 to 1.2% in December 2019.[154]

4.1.3 What is the scale and impact of ad fraud?

The prevalence of ad fraud is difficult to measure, given that some fraud will go undetected, and systems that measure fraud might throw up false positives. Furthermore, cybersecurity vendors who measure fraud use different methodologies. In consequence, estimates of the overall scale of ad fraud vary widely and there is limited UK-specific data.

Figure 4.1 shows estimates of the proportion of programmatic open display advertising impressions that are attempted fraud (fraudulent impressions put up for sale) and successful fraud (paid-for fraudulent impressions). Rates of paid-for fraud vary depending on the fraud-prevention tools used in the supply chain, with relatively low rates in the case that participants use anti-fraud verification and best practices.

[153] World Federation of Advertisers, Digital Media Benchmark, accessed 23 March 2020. Data is based on a synthesis of third-party vendor data.
[154] Digiday (January 2020). *'Definitely a concern': Influencer fraud is on the rise again on Instagram*.

Figure 4.1: Estimated rates of invalid traffic fraud

Source	Ad format(s)	Market	Fraud rate	Period	Notes
Rates of attempted fraud					
White Ops/ANA[155]	Various display/ video	USA	20% to 35%	Aug-Sep 2018	Study of 27 billion ad impressions
IAS[156]	Desktop display	Worldwide	11.7%	H1 2019	
	Desktop video		7.8%		
	Mobile web display		11.9%		
Pixalate[157]	Various display/ video	UK	11%	Q2 2019	
Rates of reported fraud (losses)					
White Ops/ANA[158]	Desktop display	USA	8%	Aug-Sep 2018	
	Desktop video		14%		
	Desktop other		12%		Includes rich media, takeovers etc.
	Mobile display		3%		
	Mobile in-app video		8%		
	Mobile web video		14%		
	Mobile other		7%		
IAS[159]	Desktop display	UK	0.9%	H1 2019	Rates refer to channels optimised against fraud.
	Desktop video		0.8%		
	Mobile web display		0.5%		
614 Group[160]	Desktop display & video; mobile web display & video.	UK, France, Germany, Italy, Netherlands	0.53%	2018	Study of 4 billion impressions in channels with end-to-end TAG certification against fraud.

Applying these fraud rates[161] to the UK programmatic open display advertising market,[162] the market we consider most susceptible to fraud, suggests that direct losses to ad fraud are in the range £7 million (supply chain fully optimised) to £100 million (one-third of the supply chain fully optimised and the rest non-optimised). Fraud losses are likely to be towards the high end of this range, given that the supply chain is not uniformly optimised across players.

However, this figure may be an underestimate. The data in Figure 4.1 is sourced mainly from anti-fraud vendors who generally focus on detecting invalid traffic generated by bot fraud and likely have a vested interest in demonstrating that their solutions work. Independent ad fraud researcher Augustin Fou believes that there are potentially "tens of billions" of dollars of fraud (globally) that is not accounted for in this data due to studies covering only well-known fraud techniques, such bot fraud.[163]

[155] White Ops / ANA (2019). *Bot Baseline, Fraud in Digital Advertising, 2018-19*.
[156] IAS (2019). *Media Quality Report*, H1 2019
[157] Pixalate (2019). *Fraud Update*, Q2 2019
[158] White Ops / ANA (2019). *Bot Baseline, Fraud in Digital Advertising, 2018-19*.
[159] IAS (2019). *Media Quality Report*, H1 2019
[160] 614 Group (2019). *TAG European Fraud Benchmark Study*, January 2019.
[161] Fraud rates could range from 0.5% (614 Group - if supply chain fully optimised across all players) to about 7.5% if two-thirds of the supply chain is optimised (based on 11% Pixalate UK non-optimised rate for 2/3 of the market and 0.5% 614 Group figure for 1/3 of the market).
[162] We estimate that the programmatic open display market was about £1.5 billion, based on CMA data (£2 billion) and an estimate of the proportion of this market that is sold programmatically (75%) taking into account that broadcaster video advertising is generally sold directly.
[163] Financial Times (30 December 2019). *Fake clicks on online ads costing companies 'tens of billions' a year*.

Click fraud is not included in the invalid traffic data, above. Researchers found an invalid pay-per-click traffic rate of 14% globally, including search and social display advertising.[164] Machine, a technology company that detects app marketing fraud, found that in the case of an anonymous gambling client, 54% of its monthly app marketing budget was spent on fraudulent app installs.[165]

The direct victims of ad fraud are advertisers who buy counterfeit advertising. Publishers are also affected due to advertisers buying counterfeit advertising instead of legitimate publisher advertising inventory. In addition to direct financial losses, ad fraud has indirect costs. A study by economist Roberto Cavazos found that these indirect costs may include less trust among industry participants, thus less innovation, and advertisers over time becoming less inclined to spend,[166] but did not quantify these effects.

The overall scale of paid-for fraud appears to be decreasing. The cybersecurity firm White Ops found that rates of fraud losses decreased from 9% in 2017 to 8% in 2019 for desktop display, and from 22% in 2017 to 14% in 2019 for desktop video.[167] IAS found that rates of non-optimised (attempted) ad fraud decreased from 14.7% in H1 2018 to 11.7% in H1 2019, while desktop video rates decreased from 9.5% to 7.8% and mobile web display increased from 9.8% to 11.9%.[168] However, fraud rates on fast-growing categories of programmatic advertising, such as mobile apps are increasing. According to Pixalate, global rates of invalid traffic fraud on mobile apps increased from 17.1% in Q3 2018 to 25.2% in Q2 2019.[169] This trend suggests that fraudsters are shifting their focus to inventory where security may be weaker. White Ops expects connected TV to be one of the fastest-growing markets for advertisers and identifies a range of ad fraud threats, including app spoofing and hidden ads.[170]

4.1.4 What are the causes of the problem?

There are numerous reasons for fraud in the programmatic open display market and these reasons are different for each type of fraud. Some of the main factors enabling fraud include:

- The market is open – in some cases, companies can access the supply chain without facing adequate vetting. Bad actors are able to participate and take cash out of the ecosystem.
- The market lacks transparency – there is limited transparency about ad trading, audiences, measurement and results. In consequence, bad actors are able to fake information about ad impressions.
- Bad actors are technologically sophisticated – fraudsters are, in some cases, able to evade the technologies market participants put in place to detect and block them.
- Anti-fraud technologies and standards used by the industry target certain categories of known fraud, such as invalid traffic or bot fraud. Fraudsters are innovative and are developing new types of fraud.
- There is limited anti-fraud validation of certain categories of ad inventory. Research by White Ops found that between 29% (mobile video bought direct) and 60% (desk video bought programmatically) were able to be validated at the highest level.[171]

[164] Professor Roberto Cavazos, *The Economic Cost of Invalid Clicks in Paid Search and Paid Social Campaigns*.
[165] https://www.machineadvertising.com/our-thinking/machine-blog/fake-clicks-on-online-ads-costing-companies-tens-of-billions-a-year-2
[166] Professor Roberto Cavazos for Cheq (2019). *Ad Fraud – The Economic Cost of Bad Actors on the Internet.*
[167] White Ops and ANA, *Bot Baseline – Fraud in Digital Advertising*, May 2019
[168] IAS, *Media Quality Report*, H1 2019
[169] Pixalate, *Ad Fraud Update*, Q2 2019
[170] White Ops and ANA, *Bot Baseline – Fraud in Digital Advertising*, May 2019
[171] White Ops and ANA, *Bot Baseline – Fraud in Digital Advertising*, May 2019

4.2 Ad misplacement and brand risk

Summary

Nature:	Brand and societal harm due to misplacement of ads on harmful content.
Scale:	Limited data about scale of misplacement of ads, but evidence of ads on harmful content.
Market:	Online display advertising and social media platforms.
Victims:	Advertisers, society and publishers.
Impact:	Brand damage, funding of harmful content, est. £167m publisher revenue lost to over-blocking.
Causes:	Presence of harmful content on the web and social media. Content verification limitations.

4.2.1 What is ad misplacement and brand risk?

Brand risk occurs when a legitimate display ad is misplaced and appears next to inappropriate content. Categories of content that are generally regarded as unsafe include adult content, hate speech, terrorism, digital piracy, military conflict, illegal drugs, crime and disinformation. However, brand safety is subjective, with many brands having their own requirements and expressing varying degrees of caution.

In the USA, the American Association of Advertising Agencies (the 4 A's) defines a brand safety floor – a recommended list of content that brands should not place ads against.[172] The floor includes the following content categories:

- Adult and explicit sexual content
- Arms and ammunition
- Crime and harmful acts to individuals and society, and human rights violations
- Death or injury
- Online piracy
- Hate speech and acts of aggression
- Military conflict
- Obscenity and profanity
- Illegal drugs
- Spam or harmful content

[172] The 4 A's, Advertising Assurance – Brand Safety Floor Framework

- Terrorism
- Tobacco, e-cigarettes and vaping
- Sensitive social issues, such as extreme political positions

However, the 4 A's provides guidance indicating that the level of risk depends on the context of content in these areas. Depiction of criminal acts is classed as high risk; dramatic depiction of criminal activity presented in the context of entertainment or news coverage is classed as medium risk; while educational, informative and scientific treatment of crime is classed as low risk.

Brand unsafe content may occur on inappropriate websites, such as sites that facilitate online piracy, or on legitimate websites and apps. In the case of the former, advertising generates revenue for the operators of these websites – financially supporting the inappropriate content and any illegal activity related to it.

The Global Disinformation Index found that disinformation content in Europe carried ads from major brands including American Express, Burger King, Dell, Made.com, O2, PayPal, Samsung, Spotify and Vodafone.[173] In one example, an ad for Amnesty International, was placed by Google on NewsFront, a Spanish disinformation site, next to an article claiming that the US blames "evil Russia" for the coronavirus outbreak.[174] In 2020, Avaaz, a campaigning group, reported that 100 brands had ads running on climate misinformation videos on YouTube, including Samsung, L'Oreal, Decathlon, WWF and Greenpeace.[175]

Figure 4.2 shows the placement of ads against a news article publicly listed by the EU vs. Disinfo website[176] as a source of disinformation. The ads displayed on this page are served by Google[177] and include a care provider, a car retailer and a bitcoin scam which uses the click bait headline "Bear Grylls Confirms Rumor". The bitcoin scam ad links through to a fake BBC news page promoting the scam. In this case, cyber criminals who run the bitcoin scam are buying advertising which funds disinformation, facilitated by Google. The scope of the project did not involve conducting a systematic review of advertising placements on disinformation content. It is possible that intermediaries other than Google also place advertising on disinformation content.

[173] Global Disinformation Index (March 2020). Ad Tech and Disinformation in the EU.
[174] Financial Times (17 March 2020). Fake news websites still profit from Google advertising.
[175] https://secure.avaaz.org/act/media.php?press_id=991
[176] https://euvsdisinfo.eu
[177] The source of the ad was identified using the AdChoices button.

Figure 4.2: Example of ad placement against disinformation content[178]

White Bullet found that branded ad campaigns, mainly for gambling companies, made up 40% of all ads served on copyright infringing websites internationally in Q4 2018, and 10% were from major brands.[179] In 2019, some major brands removed their advertising from YouTube due to placement of ads on children's videos in which paedophiles had made suggestive remarks in the comments sections.[180] In 2018, the Internet Watch Foundation found that one in ten websites dedicated to child sexual abuse host ads for legitimate brands, including some

[178] https://southfront.org/the-coronavirus-covid-19-pandemic-the-real-danger-is-agenda-id2020/ accessed on 31 March 2020
[179] https://www.white-bullet.com/q4-2018-report-10-of-all-ads-on-popular-ip-infringing-websites-in-europe-are-from-major-brands
[180] https://www.nytimes.com/2019/02/20/technology/youtube-pedophiles.html

household names. It researched a sample of 100 CSE websites of which 57 contained ads, the majority of which were for adult pornography or adult dating sites, though ads for some mainstream brands also appeared.[181]

4.2.2 What part of the industry does brand safety affect?

There is potential for misplacement of advertising against brand-unsafe content across the open online display advertising market and on social media. Advertisers generally consider risk in terms of the proximity of their ads to inappropriate content. In-stream video advertising and banner advertising is high risk because ads appear in the content. Advertising on Facebook is perceived as somewhat lower risk because ads appear in the same feed as content but are more distinct from the surrounding content. There is a lack of data about the relatively incidence of brand-unsafe content in these different parts of the market.

4.2.3 What is the scale and impact of brand safety?

Integral Ad Science, a provider of content verification technology used to prevent ad placement in inappropriate content, provides data for the percentage of pages scored that it rates as a brand risk – see Figure 4.3. IAS defines brand risk as 'Impressions on pages that are flagged for posing various levels of harm to brand image and/or reputation through association, based on eight core content categories: adult, alcohol, hate speech, illegal downloads, illegal drugs, offensive language and controversial content, and violence.[182] IAS does not define the difference between medium, high and very high risk. This data refers to the open display advertising market. Data is not available for the social display market.

Figure 4.3: Brand risk in UK online ad inventory as a proportion of pages scored, H1 2019

Category of ad inventory	High or very high risk	Medium risk	Total risk
Desktop display	0.1%	2.7%	2.8%
Desktop video	0.2%	9.6%	9.8%
Mobile web display	0.2%	3.3%	3.5%
Mobile web video	0.4%	8.9%	9.3%

Source: IAS[183]

IAS found that the percentage of pages containing risky content decreased between H1 2018 and H1 2019 in all categories except mobile web video.

Content verification services such as IAS are widely used and prevent ad placement on sites they identify as a brand risk. In consequence, the IAS data shows the level of risk brands would face if they took no action to prevent misplacement of ads, but it does not indicate the actual level of misplacement of ads.

In terms of actual placement of ads in inappropriate content, there is very limited data. In 2018, White Bullet monitored ads placed on the top 5,000 IP infringing websites, tracked across North America, Europe, Asia-Pacific and South America. It found that 10% of these ads were placed by major brands and 30% by other brands, and that 21% of ads were fraud or malware[184]. The Global Disinformation Index (GDI) estimates that $76 million of ad revenues flow to disinformation sites in Europe annually. These estimates are based on relatively crude assumptions about the price of display advertising, traffic to disinformation websites, and involve scaling

[181] https://www.gov.uk/government/news/advertisers-urged-to-help-tackle-online-child-sexual-exploitation
[182] IAS (2019). *Media Quality Report H1 2019.*
[183] IAS (2019). *Media Quality Report H1 2019.*
[184] https://www.white-bullet.com/q4-2018-report-10-of-all-ads-on-popular-ip-infringing-websites-in-europe-are-from-major-brands

up a sample, and do not take into consideration revenue share taken by intermediaries. In consequence, it is possible that the actual revenue generated by disinformation websites is substantially less than this estimate. GDI do not provide UK-specific data.

In the case that advertising appears on inappropriate content, it provides funding for this content, potentially causing societal harm. Advertisers also suffer harm to their brands. Stakeholders interviewed for this study believed that this latter harm occurred mainly when the media reported on cases of ad misplacement – causing PR damage. It is difficult to quantify this harm.

The risk of ad misplacement also has an impact on legitimate publishers, especially news publishers. Measures put in place to prevent ad misplacement, such as content verification technology and keyword block lists, may overreach and limit monetisation of legitimate content. In 2019, cybersecurity vendor Cheq estimated that of the 40% of global premium media inventory that is brand safe (neutral or uncontroversial content, not in contravention of leading advertisers' brand safety guidelines), 57% was incorrectly blocked by keywords. Block rates were especially high on LGBT stories. 73% of 30 neutral or positive articles in the Advocate and Pink News were blocked[185].

The University of Baltimore estimates that about 20% of ad revenue is lost by UK news sites due to incorrectly blocked keywords, a total cost of £167 million in 2019, including national and regional news brands and magazine brands[186]. In April 2020, Newsworks, an organisation representing UK news publishers, wrote an open letter to advertisers asking them to remove the word 'coronavirus' from their blocklists.

Newsworks estimated that the total loss to news brands of blocking online stories with the word 'coronavirus' in them would £50 million if the pandemic lasted three months[187]. However, Newsworks has not published the methodology and assumptions it used to estimate this figure. The incremental loss due to blocking of pandemic-related terms will depend on a range of factors that are, at present, unknown, including:

- Total open display advertising expenditure which may have been negatively impacted by the pandemic.
- News publisher traffic and share of the online audience which is likely to have increased due to the pandemic.
- The level of blocking of news publisher sites before and during the pandemic.

In consequence, the Newsworks figures may overestimate or, possibly, underestimate the extent of the impact of keyword blocking during the pandemic.

4.2.4 What are the causes of ad misplacement and brand risk?

The primary cause of the problem of ad misplacement and brand risk is the presence of inappropriate or harmful content on the web and social media platforms. This factor is out of scope of this study.

The secondary cause is that, in some cases, the open display advertising supply chain and social media platforms allow advertising to be placed on this content. In the open display advertising market, advertisers generally use services such as IAS to verify content and set up manual blacklists and keyword block lists. Social media platforms have proprietary approaches to determining which content is monetised by advertising. YouTube limits monetisation to channels that have more than 1,000 subscribers and 4,000 public watch hours

[185] Cheq (September 2019). Brand Safety's Technology Challenge: How Keyword Blacklists are Killing Reach and Monetization.
[186] University of Baltimore for Cheq, The Economic Cost of Keyword Blacklists for Online Publishers.
[187] https://www.newsworks.org.uk/news-and-opinion/back-dont-block-british-journalism

that also meet qualitative review criteria.[188] YouTube's 'Advertiser-friendly content guidelines'[189] determine which videos are eligible for monetisation and are more restrictive than its Community Guidelines that govern which videos are allowed on YouTube.[190] There is limited data about the effectiveness of these measures.

The problem of brand safety measures limiting news publisher advertising revenue is due mainly to the way that advertisers set up blacklists and blocklists, rather than the capabilities of content verification technology. Content verification services provide tools enabling brands to filter the web pages their ads are placed on based on a range of criteria. These services conduct proprietary analysis of web pages and offer advertisers options around the level and type of risk they wish to take. IAS uses machine learning, natural language processing (NLP) and a cognitive semantic approach to provide advertisers with options such as low/moderate/high risk and contextual relevance.[191] Cheq also uses NLP, as well as lexical semantics (understanding meaning), conversational learning and computer vision techniques.[192]

Content verification services also enable advertisers to block domains, and keywords that appear in URLs – a relatively blunt tool. Advertisers or their agencies define keyword blocklists and may, through the inclusion of certain words, limit placement of ads on news content. Following concerns around the blocking of Covid-19 related news content, the IAB has advised advertisers to take a nuanced approach to keyword blocking[193] and to back - not block - British journalism.[194]

[188] https://www.youtube.com/account_monetization?nv=1
[189] https://support.google.com/youtube/answer/6162278?hl=en-GB&ref_topic=9153642
[190] https://qz.com/1785613/how-youtube-shields-advertisers-not-viewers-from-harmful-videos/
[191] IAS, Protect and grow you brand: Brand safety & suitability
[192] https://www.cheq.ai/display-and-video#1779790716
[193] https://www.iabuk.com/news-article/CV-statement-keywords-covid19
[194] https://www.iabuk.com/news-article/covid-19-x-keyword-blocking-9-tips-advertisers

5 Regulatory framework

This section provides a high-level overview of the existing regulatory framework and the role of the ASA in relation to online advertising. The regulatory framework for online advertising is complex with instruments from across a wide range of activities. A comprehensive analysis of the legislation and regulatory structure governing all forms of advertising is outside the scope of this study.[195] The purpose of this section is to provide some context for the subsequent analysis and discussion of the various industry initiatives and measures.

The three online advertising market segments within the scope of this study – open online display, social display and influencer marketing – fall under non-broadcast advertising which is governed by the CAP Code. The existing regulatory framework for these three segments operates largely on a self-regulation basis[196] and comprises a variety of bodies involved in different aspects of regulation. There are also differences within these segments between the regulatory structures used and those with the power to sanction or enforce.

In general, the advantages and disadvantages of a self-regulatory system compared to external regulation by an independent statutory body are summarised in Figure 5.1.

Figure 5.1: Advantages and disadvantages of self-regulation

Advantages	Disadvantages
• Higher level of expertise and technical knowledge through close links between the self-regulatory body and industry. • Voluntary compliance by regulated parties who may view obligations as more reasonable and acceptable compared to externally-imposed rules. • More flexibility to facilitate timely adaptation of rules to reflect changes in the industry. • Monitoring and enforcement can also be faster which means consumers are protected sooner. • Lower regulatory costs for businesses. • Lower risk of issues of jurisdictional conflicts and legal limitations as industry codes can apply to companies who may operate across national borders.	• 'Free rider problem' – firms who do not participate gain the benefits of self-regulation without incurring costs of participation. • Potential accountability and fairness issues, though these can be addressed through various mechanisms in the design of the self-regulatory system (e.g. with reference to statutory objectives, clear statements of principles and standards, transparent procedures for complaints handling, oversight of rules by government). • Potential for imperfect outcomes or lowering of standards where there are known solutions which could be enacted through government-imposed regulations (e.g. rules on certain harmful products and services, such as cigarettes or gambling).

5.1 Legislation

There is both EU and UK legislation which applies to online advertising. Key instruments are summarised below:

- European Union: E-Commerce Directive contains various measures including rules on commercial communications such as online advertising; Audiovisual Media Service Directive, which updates rules pertaining to on demand service providers and extends certain rules to video sharing platforms (e.g. to

[195] The Competition and Markets Authority in its report on Online Platforms and Digital Advertising – Market Study Interim Report has included a more detailed Appendix on the legal framework. Available at https://assets.publishing.service.gov.uk/media/5df9ebf0e5274a0910cb6d7c/Appendix_A_The_legal_framework.pdf

[196] The ASA operates as a co-regulator alongside Ofcom for broadcast advertising in accordance with the UK Code of Broadcast Advertising (BCAP Code). The CAP Code covers advertising on VOD services which is co-regulated by the ASA and Ofcom. Advertising on VOD services is a segment of the open online display advertising market which is within the scope of this study. However, VOD advertising on TV platforms (e.g. connected TV and set-top box platforms) is not included in the scope of this study. Broadcasters voluntarily apply the BCAP Code to their VOD services.

protect children)[197]; Platform-to-Business Regulation, which applies to online intermediation service providers but not to ad-exchanges.

- Competition Law (Competition Act 1998 and Enterprise Act 2002): For protection against anti-competitive agreements or behaviours. These are based on European Union Law, which has been used in several cases concerning online advertising.
- Consumer Law: Protects consumers against unfair contract terms and unfair trading. This area of legislation applies to a wide range of matters including advertising. Again, aspects of consumer law in the UK are based on European Union Law.
- Data protection and privacy: The GDPR sets out the lawful use of data including consent, contract and legitimate interests. This is relevant to behaviour and tracking aspects of online advertising activity, and aspects of discrimination.

5.2 The ASA and its role

The ASA is the key body in the advertising industry's self-regulatory and co-regulatory system.[198] The ASA is responsible for enforcing the BCAP Code[199] for broadcast advertising and the CAP Code[200] for non-broadcast advertising, sales promotions and direct marketing. The ASA's activities include investigations and rulings on complaints, and conducting research. The CAP Code regulates the following aspects of online advertising:

- the content of marketing communications (not with terms of business or products themselves);[201]
- the impression created by marketing communications as well as specific claims, and the likely effect on consumers;
- the use of data for targeting; and
- the activity on the landing pages behind the online ads.[202]

The CAP Code does not apply to advertising that originate outside the UK and on non-UK websites. Such advertising, if targeted at UK consumers, are subject to the jurisdiction of the relevant authority in the country from which they originate. Most members of the European Union, and many non-European countries, have a self-regulatory organisation that is a member of the European Advertising Standards Alliance (EASA). EASA coordinates the cross-border complaints system for its members (which include the ASA).

The ASA attempts to seek industry compliance in the event of breaches of CAP Code for non-compliance but it does not have enforcement powers. Instead, advertisers who breach the CAP Code may be subject to sanctions which include:

- Adverse publicity from rulings published by the ASA weekly on its website;

[197] The updated AVMSD was adopted in November 2018 and is expected to be transposed into UK law by September 2020.
[198] The ASA is funded by advertisers through a voluntary levy on the cost of advertising space. https://www.asa.org.uk/about-asa-and-cap/about-regulation/our-funding.html
[199] The UK Code of Broadcast Advertising (BCAP Code) applies to all advertisements (including teleshopping, content on self-promotional television channels, television text and interactive tv ads) and programme sponsorship credits on radio and television services licensed by Ofcom.
[200] The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code) is the rule book for non-broadcast advertisements, sales promotions and direct marketing communications (marketing communications).
[201] These are subject to sector-specific regulations such as by the Medicines and Healthcare products Regulatory Agency (MHRA).
[202] To the extent that the activity relates to claims on a marketer's own website, or in other non-paid-for space online under their control (e.g. their social media accounts and apps) if they are directly connected with the supply of goods or services, opportunities, prizes or gifts.

- Denial of access to media space, whereby the CAP alerts its members to withhold their services or deny advertising space to non-compliant marketers; and
- Potential revocation, withdrawal or temporary withholding of trading privileges and recognition.

In the event of non-compliance, there is a legal backstop in the self-regulatory system which allows the ASA to refer such matters to Trading Standards for action under the Consumer Protection from Unfair Trading Regulations 2008 or the Business Protection from Misleading Marketing Regulations 2008. It is also able to refer cases to bodies with other legal powers such as the Gambling Commission and the Financial Conduct Authority.[203]

Other bodies like Citizens Advice will receive complaints and other inputs from consumers and will provide advice or refer matters to the appropriate body. The current self-regulatory structure, which has evolved over half a century,[204] inevitably creates a multi-step system, comprising both self-regulatory and other bodies. Its operation can be complex and enforcement potentially difficult and time consuming.

Other aspects of enforcement, for example criminal activity relating to fraud and scams, are not handled by the ASA but other agencies including law enforcement bodies, statutory regulators and initiatives like Action Fraud.

5.3 Standards

There are several standards initiatives for online advertising. A key body is the UK Internet Advertising Bureau. The IAB has adopted the EU Framework for Online Behavioural Advertising, which sets out good practice principles to enhance transparency and user control of targeted advertising. Other initiatives include the Joint Industry Committee for Web Standards (JICWEBS), which is seeking to reduce the risk of online advertising fraud and ads appearing in unsafe brand environments, and to maximise ad viewability.

Lastly, the EASA has developed Best Practice Recommendations (BPR) which set out a harmonised approach to self-regulation for online behavioural advertising. The 'AdChoices' Icon initiative originates from the BPR and is discussed elsewhere in this report.

[203] The ASA has memoranda of understanding with various organisations. See https://www.asa.org.uk/transparency/who-we-are-and-what-we-do.html
[204] https://www.asa.org.uk/about-asa-and-cap/our-history.html

6 Summary of industry and regulatory initiatives

There is a wide range of industry and regulatory initiatives and developments that contribute to mitigating the issues of inappropriate ad content, inappropriate ad targeting, ad fraud and brand safety risk. The mode of action of these initiatives ranges from provision of technology to enable the detection of malware, fraud and unsafe pages, through to industry standards that encode the use of this technology – and define related processes. Consumer literacy campaigns educate the public about potential harms, while consumer tools and settings enable consumers to turn off certain forms of online advertising encouraging the industry to deliver advertising consumers accept. ASA initiatives increasingly include proactive monitoring involving innovative technology-driven research techniques. Figure 6.1 provides a summary of the key industry initiatives.

Figure 6.2: Summary of relevant industry and regulatory initiatives and developments

Category of initiative / development	Mode of action	Initiative / development	Description
1. Industry standards and best practice	Coordinate industry participants to use best-practice technology and processes to fight bad ads and fraud and ensure brand safety.	IAB Gold Standard	• Umbrella standard incorporating JICWEBs DTSG brand safety (below), ads.txt (helps combat fraud), and LEAN principles (ad user experience).
		TAG Certified Against Malware	• Self-regulatory standards to combat malware in the open display advertising ecosystem.
		TAG Certified Against Fraud	• Self-regulatory standards to combat fraud in the open display advertising ecosystem.
		JICWEBs DTSG brand safety	• Self-regulatory standards to reduce risk of brand misplacement in open display and on social platforms.
		EDAA AdChoices	• Icon providing consumers with information about online ads and targeting.
2. Platform rules and policies	Set parameters for advertiser content and practices.	Various, such as Facebook and Google	• Rules and policies developed by platforms to govern the use of advertising, including prohibitions and limitations on various advertising content and practices.
3. Technology solutions	Provide a level of protection against security threats and screen for bad ads and targeting.	Cybersecurity solutions	• Proprietary and third-party software that detects and blocks malvertising, fraud or brand-unsafe content.
		Distributed ledger technology	• JICWEBs DLT pilot is a closed network within the open display ad market with potential to reduce fraud.
4. Consumer media literacy campaigns	Raise consumer awareness and literacy of the risks of harm and preventative measures.	AA Media Smart	• Awareness campaign that helps 7- to 16-year olds to be "critical consumers of media".
		ICO Be Data Aware	• Awareness campaign to help consumers understand how their personal data is being used and why.
5. Consumer tools and services	Enable consumers to switch off advertising and/or targeting as "last resort", eliminating risk of harms.	Service settings/features	• Facebook and Google features enabling consumers to limit personalised advertising on their services.
		OS and browser ad controls	• Browser features that limit personalised advertising as a default or as an option.
		Ad blockers	• Software that limits online advertising shown on a browser – at its limit, blocking advertising.
6. ASA monitoring and best practice initiatives	Complements complaints-based system with proactive identification of issues.	ASA Avatars	• Research using computer programmes to mimic human behaviour and identify ads shown to children.
		Emerging ASA initiatives	• New initiatives such as avatar monitoring of children in mixed-age audiences and monitoring of logged-in environments – social media services.

There are a large number of industry and regulatory initiatives relevant to the issues of inappropriate advertising, ad fraud and brand safety. However, in many cases the primary purpose of these initiatives is to

address other problems and the impact on these issues is incidental. In addition, platform rules and policies prohibit most forms of harmful advertising but their effectiveness depends on platform enforcement measures.

Figure 6.3 shows the main initiatives, the issues addressed and whether these are the primary purpose of the initiative.

Figure 6.3: Issues addressed by industry and regulatory initiatives

Category	Initiative / development	Issues addressed				
		Malvertising	Bad content	Bad targeting	Ad fraud	Brand safety
1. Industry standards and best practice	IAB Gold Standard				●	●
	TAG Certified Against Malware	●				
	TAG Certified Against Fraud				●	
	JICWEBs DTSG brand safety					●
	EDAA AdChoices		○	○		
2. Platform rules and policies	Various	●	●	●	●[205]	●[206]
3. Technology solutions	Cybersecurity solutions	●	●		●	●
	Distributed ledger technology	○			○	
4. Consumer media literacy campaigns	AA Media Smart		○	○		
	ICO Be Data Aware			○		
5. Consumer tools and services	Service settings/features			○		
	Browser ad controls			○		
	Ad blockers	○	○	○		
6. ASA monitoring and best practice initiatives	ASA Avatars			●		
	Emerging ASA initiatives	●	●	●		

Key:
● Initiative specifically directed at solving or mitigating the issue.
○ Initiative has an impact on the issue, but it was established to address other problems/issues

The issues of inappropriate advertising, ad fraud and brand safety are addressed unevenly by industry and regulatory initiatives – and the effectiveness of these initiatives differs.

- **Malicious advertising (malvertising)** is mitigated by the TAG Certified Against Malware programme of best practice, and cybersecurity solutions which may be used within or outside of this programme. Take up of the TAG scheme is lower than TAG Certified Against Fraud and the IAB Gold Standard.[207] Some industry interviewees attributed this difference to open display advertising supply chain participants prioritising action on other issues, such as GDPR and brand safety. Industry stakeholders suggest that the cybersecurity solutions do not detect all malicious advertising. There is a lack of industry standards

[205] Online display advertising intermediaries generally have rules and policies that prohibit fraudulent practices such as the sale of invalid impressions or reselling inventory without the permission of the owner.
[206] Platforms have rules and policies governing content shared by users, which help to ensure brand safety. These rules are not within the scope of this study.
[207] Plum analysis of adoption of schemes by DSPs and SSPs in terms of market share – see Sections 7.1, 7.2 and 7.3.

on aspects of the problem such as vetting of ad buyers and identifying ad creative consistently throughout the supply chain.

- Other forms of **inappropriate ad content**, such as offensive advertising or advertising for illegal and counterfeit goods, are tackled mainly by supply chain participants' proprietary technology and processes which differ between companies. Although the advertising codes set content standards, there are no self-regulatory standards or initiatives setting out best practice for vetting buyers, the process of scanning ads for inappropriate content, or taking and handling reports and complaints. In some vendor implementations of interstitials[208] behind the AdChoices icon, reporting of inappropriate content is enabled, though this is not a stated aim of AdChoices. Media literacy campaigns may help consumers learn to identify inappropriate ad content when they see it, but this is not their main objective. The ASA complaints-based system is the main form of self-regulation in this area, though the ASA is developing its capacity to proactively identify issues in certain areas.

- **Inappropriate targeting** of advertising is to some extent covered by media literacy initiatives and AdChoices, which make consumers aware of how, in general, online advertising is targeted to them. Platform and browser settings provide consumers with the ability to limit personalised targeting. The advertising codes cover mis-targeting of certain categories of advertising to children and the ASA avatars initiative is increasing proactive detection of breaches in this area - to supplement the complaints-based system. Discriminatory targeting and targeting of vulnerable audiences are not well codified at present and there are no industry best practice initiatives in this area, though the ASA has initiated research on this topic.

- **Ad fraud** is mitigated by the TAG Certified Against Fraud programme of best practice, and cybersecurity solutions which may be used within or outside of this programme. Take up of the TAG scheme covers over 80% of the open display advertising intermediary market by value.[209] The IAB Gold Standard requires adoption of ads.txt which helps limit fraud but is just one of the many elements of the TAG scheme. A study found that end-to-end TAG certification in the supply chain reduces fraud by 94%, though this includes only invalid traffic fraud and does not include any undetected fraud.

- **Brand safety risk** is mitigated by the JICWEBS DTSG brand safety standards that are relatively widely adopted by buyers and publishers and a requirement for IAB Gold Standard accreditation. These standards require adoption of content verification technology or schedules. The effectiveness of the JICWEBS DTSG standards is difficult to determine due to a lack of measurement and variation of brand safety objectives and tolerance by brand. Data from content verification vendor IAS suggests that between 3.5% (mobile display) and 9.8% (desktop video) of web pages scored involve brand risk which is blocked if this vendor is used to comply with the standards.

6.1 Incentives and mechanisms of the current self-regulatory system

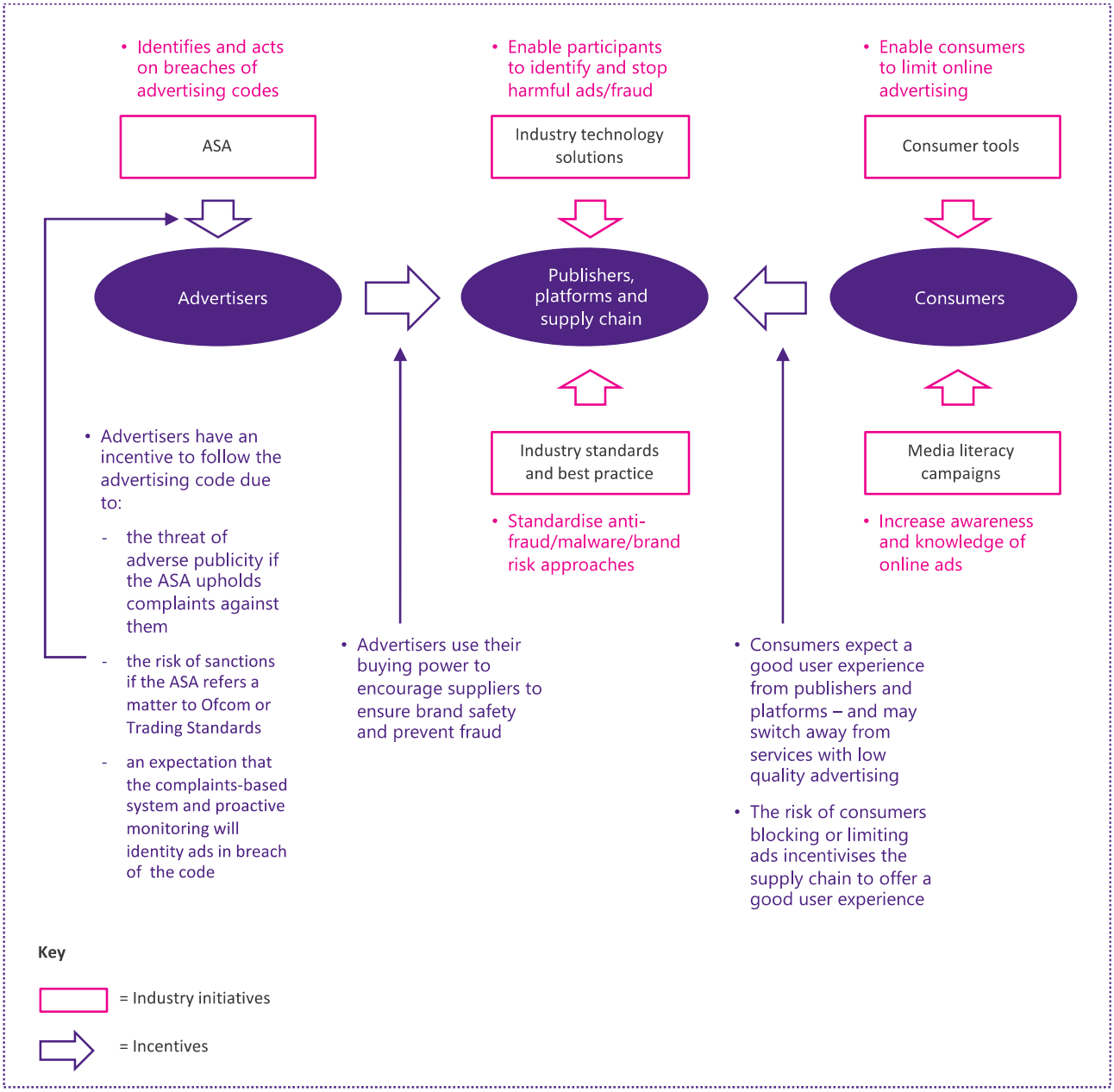
The current self-regulatory system is based on a set of incentives for market participants to comply with CAP Code regulation, and a set of industry bodies, initiatives and market developments to support and encourage compliance. Figure 6.4 illustrates this system. At a high level:

- Advertisers are incentivised to comply for reputational reasons – to avoid the risk of brand damage from running inappropriate advertising and being caught out.

[208] An interstitial is a web page displayed before or after an expected content page, usually to display advertisements. Most interstitial advertisements are delivered by an ad server.
[209] Plum analysis of the market share of DSPs and SSPs that have adopted the programme using data provided in the CMA Online platforms and digital advertising market study interim report, Appendix C.

- The supply chain – including agencies, social media platforms, open display market intermediaries and publishers – is incentivised by pressure from its advertiser and consumer customers. Advertisers want to prevent brand risk and fraud. They can, to some extent, use the threat of switching suppliers to exert this pressure. Consumers want a good user experience and quality advertising. In cases where they have a choice of publisher or platform, they may favour services that provide a good experience. In addition, they may limit online advertising by using an ad blocker or changing service settings.

Figure 6.4: Online advertising self-regulatory system



This system of incentives has certain limitations:

- The reputational incentive for advertiser compliance works in the case of advertisers who care about their brand reputation but is likely less effective in the case of advertisers who are bad actors with the intention to engage in harmful activity.[210]

- The reputational incentive for advertiser compliance based on the risk of adverse ASA rulings works if advertisers believe that non-compliant ads will be detected. The probability of consumers noticing and reporting inappropriate ads increases with the scale of an ad campaign. Small-scale advertisers may have a low incentive to comply if they expect any non-compliant ads not to initiate complaints.

- The incentive based on the risk of sanctions if the ASA refers an advertiser to Trading Standards or other statutory bodies works for UK-based advertisers but may be limited for overseas advertisers, though EASA operates a cross-border complaints system.[211]

- Advertiser pressure on the supply chain relates mainly to brand safety and ad fraud and has a more limited influence on consumer issues such as inappropriate advertising.

- Consumer and advertiser pressure may have limited impact on the open display advertising supply chain, given the complexity of this market – incentives need to feed through between participants at different levels of the supply chain. For example, a publisher has an incentive to provide a good user experience but must rely on its suppliers such as SSPs to deliver quality, malware-free advertising.

- Consumer and advertiser pressure may have more limited effect in the case of a platform with market power, such as Facebook in social display advertising. Though we did not find evidence for a lack of measures to prevent inappropriate advertising relative to other platforms.

- To some extent, the incentives depend on a strong feedback loop between consumers, regulators and advertisers. However, unclear and fragmented mechanisms for reporting inappropriate advertising may weaken these incentives. There is also a lack of clarity in how complaints are dealt with by different agencies and platforms which could deter consumers from raising complaints.

- Some aspects of harm may have a low impact at an individual level (e.g. misleading ads) or are not obvious to consumers (e.g. inappropriate or discriminatory targeting) which makes it difficult for consumers to play an active role in providing feedback or complaints which is an important feature of a self-regulatory system.

Where industry participants do have an incentive to comply with regulation, the self-regulatory measures to prevent inappropriate advertising, ad fraud and brand safety risk may be limited. In particular:

- Industry technology solutions help to prevent ad fraud, brand safety risk, malicious advertising and to screen ad creative for inappropriate ads. But these technologies do not prevent all inappropriate activity.

- Industry standards initiatives define certain processes and measures, and generally set a minimum requirement, with a risk of levelling down.

The following sections describe each of the initiatives listed above in terms of objectives and issues addressed; how it works; uptake or reach; drivers and barriers to adoption; and future developments.

[210] An example is in direct marketing segment where the Digital Economy Act 2017 introduced a sanctions mechanism with heavier fines to address an issue of concern relating to unsolicited nuisance calls. https://www.gov.uk/government/news/no-escape-for-company-bosses-responsible-for-nuisance-calls

[211] https://www.easa-alliance.org/coverage/cross-border-complaints-system

7 Industry standards and best practice

7.1 IAB Gold Standard

The IAB Gold Standard is a broad industry standards initiative which addresses three specific areas – ad fraud, brand safety and digital advertising experience. It is targeted at companies operating within display advertising on desktop and mobile web. Certification requires demonstration of compliance to other industry-led programmes or standards in the three areas. Thus, there is some overlap with other initiatives on fraud (TAG) and brand safety (DTSG) which are discussed in the subsequent sections below.

7.1.1 Objectives

The IAB Gold Standard[212] is an industry standards initiative launched in October 2017 by the Internet Advertising Bureau (IAB UK), with a revised Standard 1.1 launched in April 2019.[213] It has three 'simple but fundamental' aims:

- **To reduce ad fraud –** companies registered or certified for the IAB UK Gold Standard should demonstrate support for or through implementation of IAB Tech Lab's ads.text project.[214] It aims to increase transparency of programmatic advertising and allows publishers and distributors (domain owners) to publicly declare the companies authorised to sell their digital inventory in order to prevent the sale of spoofed or fake inventory.

- **To increase brand safety –** current non-signatories are expected to become certified signatories to the JICWEBS Digital Trading Standards Group (DTSG) Brand Safety Principles,[215] and current signatories should continue to have their policies and processes independently verified; and

- **To improve the digital advertising experience –** registered and certified companies should adhere to the standards set by the Coalition for Better Ads.[216] The Coalition for Better Ads has developed Better Ads Standards for desktop web and mobile web based on consumer research. The Standards for North America and Europe were published in March 2017, and the Coalition for Better Ads announced support for the same Standards to be adopted worldwide for desktop and mobile web.

There is no cost for members' participation in the IAB UK Gold Standard; however, there are financial costs associated with certification for the JICWEBS DTSG.

Further information on the sub-initiatives that organisations must comply with are outlined in Figure 7.1.

[212] https://www.iabuk.com/goldstandard
[213] https://www.iabuk.com/sites/default/files/public_files/Gold-Standard-1.1.pdf
[214] ads.txt stands for 'Authorized Digital Sellers'. https://iabtechlab.com/ads-txt-about/
[215] Further information on certification and associated costs for JICWEBS DTSG are outlined on the JICWEBS website: https://jicwebs.org/certification-process/become-certified/
[216] For further information, refer to: https://www.betterads.org/standards/

Figure 7.1: Information on Gold Standard sub-initiatives from IAB Tech Labs, JICWEBS, and Coalition for Better Ads

Ad fraud reduction – IAB Tech Lab's ads.txt[217]

ads.txt (Authorized Digital Sellers) aims to increase transparency in programmatic advertising by offering publishers and distributors a flexible and secure method to publicly declare the companies they authorised to sell their digital inventory. ads.txt creates a public record of Authorized Digital Sellers and intends to give publishers greater oversight and control over their inventory and to make it harder for bad actors to profit from selling counterfeit inventory.

Increase brand safety – JICWEBS DTSG Brand Safety Principles[218]

DTSG was established in 2012 with the aim of developing industry-led guidelines to reduce the risk of misplacement of advertising across the digital trading ecosystem. There are seven key DTSG Good Practice Principles, which form the basis of JICWEBS Brand Safety certification. These include:

- Buyers and sellers of digital display and audio advertising shall ensure that the transaction follows a Primary Agreement or Contract.
- The Primary Agreement or Contract should include where advertising should (or should not) appear, using independently certified Content Verification (CV) tools.
- Sellers of directly and indirectly sourced inventory should confirm how they minimise the risk of ad misplacement.
- Sellers should be able to explain the process(es) that minimise risk of ad misplacement.
- Sellers should have policies in place to appropriately respond to ad misplacement via takedown, and processes to enact these policies.
- Buyers and sellers should have a nominated Responsible Officer for JICWEBS DTSG Brand Safety issues.
- An independently verified JICWEBS-approved provider will review each Signatory's ad misplacement minimisation policies.

Improve digital advertising experience – Coalition for Better Ads' standards[219]

The Better Ads Standards for desktop web and mobile web were developed based on research of more than 66,000 consumers. The Standards for North America and Europe were published in March 2017, and worldwide adoption of the same Standards for desktop web and mobile web was proposed by the Coalition in January 2019. In January 2020, the Coalition also announced a Standard for short-form video.

The research undertaken to identify and define Better Ads Standards found 14 web-based ad formats associated with poor consumer experience. These included desktop web experiences (pop-up ads, auto-playing video ads with sound, prestitial ads with countdown, and large sticky ads), mobile web experiences (pop-up ads, prestitial ads, ad density higher than 30%, flashing animated ads, auto-playing video ads with sound, postitial ads with countdown, full-screen scroll over ads, and large sticky ads), and short-form video experiences (long pre-roll ads that cannot be skipped, mid-roll ads, and large display ads).

7.1.2 Description of initiative

There is a two-stage certification process for companies wishing to join the IAB UK Gold Standard, and eligibility is limited to organisations operating within display-only advertising.[220]

The first stage of the certification process is for an organisation to register for the Standard via an online questionnaire. In the case of organisations with several different businesses (as categorised in Figure 7.2), a

[217] https://iabtechlab.com/ads-txt/
[218] https://jicwebs.org/standards/brand-safety/
[219] https://www.betterads.org/standards/
[220] This includes direct and indirect sellers, buyers, buyer support, other support functions such as facilitating DSPs or exchanges.

separate registration form will need to be completed for each type of business that will enter the Standard. For example, two separate registrations would be required for an organisation operating an ad exchange and a consumer-facing website. Registered organisations will be issued with the IAB UK Gold Standard 'Registered' badge that can be placed on their website and marketing materials.

Figure 7.2: IAB UK Gold Standard business categories

- Direct Sellers (owned inventory)
- Indirect Sellers (non-owned inventory)
- Support (tech platforms and services)
- Buyer Support Companies (buy inventory on behalf of brands and agencies)
- Buyer Companies (purchase directly or as a representative of another company)
- All other (Data, Quality, Creative)*

Note: *other business categories may include companies that provide ad verification, creative industries, content management platforms, DMPs, etc. Source: IAB

The second stage is to complete the certification process, to be fully Gold Standard Certified. Registered organisations have six months to submit the requested information relevant to their business category to IAB UK for review.[221] The IAB UK Gold Standard 1.1 guidance details information on evidence requirements for each business category (as noted in Figure 7.2).[222]

The current Standard version is IAB UK Gold Standard 1.1, which requires organisations to be fully certified under the JICWEBS DTSG for Brand Safety before they can receive Gold Standard accreditation. The Standard version 1.1 also introduced the requirement for organisations to complete IAB UK Gold Standard training offered by IAB's dedicated training platform, and introduced thresholds for support of the ads.txt, Coalition for Better Ads principles and the 'Better Ads Standards'. There were also additional requirements for specific business categories; for example, buy-side and sell-side platforms must ensure that 90% of traffic they deliver includes a valid ads.txt file.

7.1.3 Adoption

As of March 2020, the Gold Standard 1.1 is adopted by 105 (over 60%) out of some 160 IAB UK members for whom the Gold Standard is applicable. Figure 7.3 shows the current list of certified members. The IAB's target is for all members to be certified. The Gold Standard is adopted by all of the main media agency groups and independents, about 81% of the DSP market by value, about 80% of the SSP market,[223] as well as many major UK media owners and global owned and operated platforms, such as YouTube, Facebook and Amazon.

Since the introduction of Gold Standard 1.1, the IAB noted that around 30 members had applied but did not complete the process due to the technical requirements for certification.

[221] IAB's process is subject to external audit by the Audit Bureau of Circulations (ABC).
[222] Refer to: https://www.iabuk.com/sites/default/files/public_files/Gold-Standard-1.1.pdf
[223] Plum analysis of data provided in the CMA Online platforms and digital advertising market study interim report, Appendix C.

Figure 7.3: Gold Standard Certified and Registered companies

Direct sellers (owned inventory)	Indirect sellers (non-owned inventory)	Support (Tech platforms & services)	Buyer Support	Buyers
• Amazon Advertising (1.1) • DAZN Media (1.1) • The Guardian (1.1) • Hello! (1.1.) • Hearst UK (1.1) • Immediate Media (1.1) • LADBible Group (1.1) • Mail Metro Media (1.1) • News UK (1.1) • Telegraph Media Group (1.1.) • TI-Media (1.1) • TripAdvisor (1.1) • Verizon Media (1.1) • Vevo (1.1) • Auto Trader (1.0) • Bauer Media UK (1.0) • ESI Media (1.0) • Facebook (1.0) • Google, YouTube (1.0) • Haymarket Automotive (1.0) • Instagram (1.0) • Reach (1.0) • Samsung Ads (1.0) • Spotify (1.0) • The Student Room (1.0) • Sky Sports and News (Registered) • Twitter (Registered)	• Exponential (1.1) • GumGum (1.1) • Index Exchange (1.1) • Inskin Media (1.1) • JustPremium (1.1) • Precise TV (1.1) • Rezonence (1.1) • Rubicon project (1.1) • Smadex (1.1) • Sovrn (1.1) • Teads (1.1) • TI-Media (1.1) • TripleLift (1.1) • Venatus Media (1.1) • Verizon Media (1.1) • AdColony (1.0) • Adform (1.0) • Flowplayer (1.0) • Mapp Media (1.0) • Mobsta Ltd (1.0) • Nano Interactive (1.0) • Ogury (1.0) • Sublime (1.0) • Tan Media (1.0)	• Amazon Advertising (1.1) • Blis (1.1) • Crimtan (1.1) • Encore Digital Media (1.1) • Pubmatic (1.1) • Quantcast (1.1) • Smadex (1.1) • SYZYGY (1.1) • Verizon Media (1.1) • Xandr (1.1) • Adform (1.0) • Adverty (1.0) • ADYOULIKE (1.0) • Encore Digital Media (1.0) • Exponential (1.0) • Google – AdX (1.0) • Nano Interactive (1.0) • Nativo (1.0) • OpenX (1.0) • Playbuzz (1.0) • SBDS Group (1.0) • Scoota (1.0) • TAN Media (1.0) • Verizon Media DSP (1.0) • Cavai (Registered) • SpotX (Registered) • The MediaGrid (Registered) • The Trade Desk (Registered)	• Capity Technologies Limited (1.1) • Havas (1.1) • MiQ (1.1) • Omnicom Media Group UK (1.1) • Publicis Media (1.1) • Audience Store (1.0) • Cadreon (1.0) • Nativo (1.0) • the7stars (1.0) • Unruly (1.0) • Xaxis (1.0) • Dentsu Aegis Network, Amnet UK (Registered)	• Agenda21 (1.1) • Amazon Advertising (1.1) • Havas (1.1) • Omnicom Media Group UK (1.1) • The Kite Factory (1.1) • MediaCom North (1.1) • Spiritmedia Scotland Ltd (1.1) • SYZYGY (1.1) • Total Media (1.1) • GroupM Digital Programmatic Services (1.0) • IPG Mediabrands (1.0) • the7stars (1.0) • The Media Shop Scotland (Registered)

Note: IAB UK Gold Standard certified and registered companies, as of 30 March 2020. Gold Standard certification status is noted in brackets.
Source: https://www.iabuk.com/news-article/gold-standard-certified-and-registered

7.1.4 Efficacy

There is no formal tracking by IAB of the overall efficacy of the Gold Standard in meeting its stated objectives. As the underlying sub-initiatives are independent of the Gold Standard itself, any improvements will be due to the effectiveness of the individual initiatives themselves rather than the Gold Standard. However, to the extent that the Gold Standard raises industry awareness of and adherence to these sub-initiatives and associated standards, it could contribute to addressing some of the issues of ad fraud and brand safety.

The IAB has noted that the implementation of the Better Ads Standards has coincided with a decline in ad blocker usage rates[224] although it is not evident that this is a direct result of the adoption of the Gold Standard.

[224] IAB response to Call for Evidence.

In any event, better user experience arising from improved ad formats does not address the specific consumer issues highlighted in Section 3.1 above.

7.1.5 Drivers of and barriers to adoption

The main driver of adoption of the IAB Gold Standard is the recognition that it provides to industry participants across the online advertising value chain. The IAB notes that it is often the buyers who drive adoption across the rest of the downstream players in the value chain. With the certification, these players would have a competitive advantage in terms of vying for advertisers.

Some potential barriers include the audit costs associated with adherence to the JICWEBS/DTSG standards, the resource commitment to meet the technical requirements (typically 6 months).

7.1.6 Future developments

In January 2020, IAB UK announced that Gold Standard 2.0 will be introduced in Q4 2020. This will incorporate IAB Europe's Transparency & Consent Framework (TCF version 2.0); the compliance criteria for incorporating the TCF within the Gold Standard certification are yet to be agreed. The TCF is an industry-led industry-standard based GDPR consent solution. Its objective is to assist all businesses in the digital advertising supply-chain comply with the EU's GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device (tracking technology such as cookies, advertising identifiers, device identifiers and others). The inclusion of the TCF does not impact on the issues in this study.

As part of Gold Standard 2.0, IAB UK also plan to introduce an independent third-party to audit the certification process. Revisions to the Gold Standard versions have been developed by IAB UK with input from the Gold Standard Group, a cross-industry committee of IAB UK members that make key decisions on Gold Standard issues.[225]

7.2 TAG Certified Against Malware programme

The TAG Certified Against Malware programme sets best practice guidelines with the aim of eliminating the distribution of malware through the digital advertising value chain. It has moderate levels of adoption among UK open display advertising market participants, but there is a lack of evidence about the efficacy of the programme.

7.2.1 Objectives

The Trustworthy Accountability Group (TAG) is a US-based cross-industry programme focusing on eliminating fraudulent digital advertising traffic, combating malware, fighting ad-supported internet piracy and promoting brand safety. JICWEBs works closely with the US-based Trustworthy Accountability Group (TAG) to align standards across the UK and the USA. JICWEBs provides certification of TAG schemes in the UK.

TAG established the Certified Against Malware programme with the objective of eliminating the distribution of malware throughout the digital advertising value chain. TAG defines malware as any malicious software impacting a computer or device without user consent, such as spyware, bots, viruses, adware, phishing and

[225] Gold Standard Group members include Accenture, Adcolony, Bauer, Exponential, Facebook, Google, GroupM, Index Exchange, Inskin, MGOMG, MMM, NewsUK, OMG, OpenX, Publicis, Quantcast, Shpock, Spark Foundry, Teads, The Guardian, Verizon, and Xandr. https://www.iabuk.com/standard-content/gold-standard

auto-subscription, with examples of malware events including auto-redirecting, drive-by-download (users unintentionally download malicious software) and deceptive download (users authorise a download but malicious software is also downloaded).

7.2.2 Description

The Certified Against Malware programme sets best practice guidelines for industry participants including direct sellers, intermediaries, buyers and vendors. Companies that are shown to follow the Certified Against Malware Guidelines receive the Certified Against Malware seal. TAG also provides tools to aid compliance with its guidelines.

The main action of the programme is to ensure that compliant companies scan ads and landing pages to screen out malware and share information with other participants to deal with malware incidents. The requirements set out in the guidelines differ by category of participant. The main elements include:

- **Documenting points of contact at partner companies** in order to enable rapid notification and escalation of malware issues.
- **Documenting and performing scans of assets and landing page URLs.** Legal agreements with supply chain partners must assign responsibilities for scanning. Relevant participants must conduct an initial scan of a 'reasonable percentage' – in practice 100% - of ad campaign assets and landing pages prior to delivery (before ads are run) following practices specified in TAG Technical Best Practices Against Malware. They must also re-scan active campaign assets and landing pages with 'reasonable frequency'. Participants must investigate and attempt to remediate any malware identified in initial scans and re-scans.
- **Putting in place procedures for handling incidences of malware.** Participants must employ procedures to deal with "red flag" events – malware incidents that are significant in terms of revenue impact, consumer experience and/or sophistication. Notification of supply chain partners must be immediate.
- **Employing Seat ID to handle malware incidents.** Seat ID is a persistent buyer identity that flows through the supply chain, enabling the supply chain participants to communicate and switch off troublesome buyers.
- **Post-mortem investigations of incidents** to ensure that knowledge is shared and learned from.

Companies must become a TAG member and pay a participation fee in order to be eligible for participation in the Certified Against Malware programme. Certification is done through independent validation or self-attestation. The company provides binding attestations that it is in full compliance with the guidelines. Additional requirements include designating a TAG Compliance Officer within the company, attending training, and quarterly internal reviews of compliance. The seal must be recertified annually.

7.2.3 Adoption

23 companies are TAG Certified Against Malware compliant, including two malware detection vendors, and 21 buyers, sellers and intermediaries[226]. The seal is held by:

[226] https://www.tagtoday.net/certified-against-malware-compliant-companies/

- 4 of the top 10 DSPs by UK market share, which we estimate account for about 75% of the UK programmatic display ad market by value[227].
- 5 of the top 12 SSPs, which account for about 70% of the market.

Several major DSPs and SSPs are not certified, such as The Trade Desk, Adobe, AdForm, Rubicon Project, Pubmatic and Triplelift – as well as many smaller players.

7.2.4 Drivers of and barriers to adoption

Industry participants interviewed for this project believed that the main reasons for relatively low levels of adoption of Certified Against Malware are a lack of awareness of the malvertising issue and a prioritisation of issues that regulators or clients require action on, such as GDPR and brand safety respectively. The cost of TAG membership and certification, and the resources required to implement Certified Against Malware may also present a barrier.

7.2.5 Efficacy

TAG has not conducted research into the efficacy of Certified Against Malware. However, some industry participants believe that Certified Against Malware is making a valuable contribution to the fight against malicious advertising. '*Industry initiatives like TAG's Certified Against Malware program, which have increased general awareness around the threat of malware and galvanized efforts to combat it*'.[228]

We do not have information about the anti-malware practices of supply chain participants who have not adopted Certified Against Malware. However, data from Confiant (see Section 3.4.1) suggests that certain SSPs – possibly those not Certified Against Malware – have high rates of malvertising relative to other SSPs.

7.2.6 Future developments

TAG recently launched a malware threat-exchange, a means of sharing information about malware threats in real time. This development is intended to reduce the time required to identify and take down malware incidents.

7.3 TAG Certified Against Fraud programme

The TAG Certified Against Fraud programme sets best practice guidelines to combat invalid traffic (IVT) in the digital advertising supply chain. It has moderate levels of adoption among UK open display advertising market participants. A study shows that the programme is effective in reducing IVT[229], but its analysis uses non-independent data. The programme does not tackle other forms of ad fraud, such as click fraud.

[227] Plum analysis of data provided in CMA (2019). *Online platforms and digital advertising market study.* Interim Report. Appendix C.
[228] Confiant (2019). *Demand Quality Report for Q3 2019.*
[229] 614 Group commissioned by TAG (January 2019). *TAG European Fraud Benchmark Study*.

7.3.1 Objectives

TAG established the Certified Against Fraud programme in 2016 to combat invalid traffic in the digital advertising supply chain. In the UK, JICWEBS adopted the TAG Certified Against Fraud programme to replace its own Anti Ad Fraud scheme from January 2019.[230]

7.3.2 Description

The Certified Against Fraud programme sets best practice guidelines for industry participants including direct sellers, direct buyers, intermediaries and anti-fraud and measurement services. Companies that are shown to follow the Certified Against Fraud Guidelines receive the Certified Against Fraud seal. TAG also provides tools to aid compliance with its guidelines.

The main action of the programme is to filter traffic for invalid traffic and to implement Payment ID and ads.txt. The requirements set out in the guidelines differ by category of participant. The main elements include:[231]

- Having a designated TAG compliance officer;
- Attending 'Certified Against Fraud' annual training;
- Complying with Detection and Filtration guidelines. The company must use either in-house technology or a third-party vendor that either achieves Media Rating Council (MRC) accreditation for digital services, including general invalid traffic detection and filtration, or is certified by an independent auditor that fraud detection and measurement capacities are compliant with the GIVT provisions of the MRC IVT Detection and Filtration Guidelines Addendum. The requirements permit the use of sampling methodology – applying detection and filtration to a sample of impressions, not 100% of impressions;
- Employing domain threat filtering and IP threat filtering to cut out websites that have been identified as high risk. There is an exception for mobile in-app inventory;
- Employing data centre IP threat filtering to cut out IP addresses that have been identified as high risk of being invalid traffic. The TAG Data Centre IP List is available to assist companies in meeting this requirement;
- Implementing Publisher Sourcing Disclosures. Direct sellers must disclose their paid traffic sourcing practices – paying third parties for visits to its websites or other media properties, such as paid email marketing, social media and affiliate links. They must also disclose the percentage of visits acquired through paid traffic sources;
- Implementing the Payment ID System; and
- Implementing Ads.txt, an IAB standard that communicates which intermediaries are authorised to sell a particular publisher's inventory, to avoid practices such as domain spoofing.

Companies must become a TAG member and pay a participation fee in order to be eligible for participation in the Certified Against Fraud programme. In the UK, certification is done through independent validation. The company submits binding attestations that it is in full compliance with the guidelines and the independent validator audits these attestations.

[230] https://jicwebs.org/standards/ad-fraud/
[231] TAG Certified Against Fraud Guidelines, Version 4.0, January 2019

TAG provides companies with the following tools to aid in compliance:

- Payment ID System - a chain of custody for digital advertising transactions, helping companies to ensure that payments made in the digital ad ecosystem are going to legitimate partners.
- Data Centre IP List - a common list of IP addresses with invalid traffic coming from data centres where human traffic is not expected to originate.
- Publisher Sourcing Disclosure Requirements (PSDR) - this policy tool outlines the requirements for publishers to disclose the volume of traffic acquired through paid sources.
- Ads.txt Specification - creates greater transparency in the inventory supply chain by creating a public record of Authorized Digital Sellers, giving publishers greater control over their inventory in the market, and making it harder for bad actors to profit from selling counterfeit inventory across the ecosystem.

7.3.3 Adoption

Presently 139 companies are TAG Certified Against Fraud compliant which break down as follows in Figure 7.4.

Figure 7.4: : Breakdown of TAG Certified Against Fraud compliant companies by category, March 2020

Category of company	Number
Buyer	10
Buyer & Direct Seller	5
Buyer & Intermediary	4
Buyer, Intermediary & Direct Seller	2
Direct Seller	53
Direct Seller & Intermediary	5
Fraud Detection Vendor	4
Fraud Detection Vendor & Measurement Service	2
Intermediary	52
Measurement Service	2

Source: TAG[232]

In terms of intermediaries in the UK, the Certified Against Fraud seal is held by:

- 6 of the top 10 DSPs by UK market share, which we estimate account for about 81% of the UK programmatic display ad market by value.[233]
- 7 of the top 12 SSPs, which account for about 83% of the market.

[232] https://www.tagtoday.net/certified-against-fraud-programcompliantcompanies/ accessed 20 March 2020
[233] Plum analysis of data provided in CMA (2019). *Online platforms and digital advertising market study. Interim Report,* Appendix C.

Several major DSPs and SSPs are not certified, such as The Trade Desk, Adobe, Verizon, Rubicon Project and Xandr – as well as some smaller players. It is possible that these companies use approaches that meet or exceed the requirements of the TAG programme, or alternative robust approaches, but have not become certified.

7.3.4 Drivers of and barriers to adoption

Industry participants interviewed for this project believed that one of the main reasons for certain companies not to adopt Certified Against Fraud is a lack of prioritisation of action on fraud relative to other issues, such as GDPR and brand safety. The cost of TAG membership and certification, and the resources required to implement Certified Against Fraud may also present a barrier.

7.3.5 Efficacy

In 2018, the 614 Group conducted quantitative and qualitative research that measured the impact of TAG Certification in reducing ad fraud. The research was conducted in the UK, France, Germany, Italy and the Netherlands. The research analysed a sample of 4 billion ad impressions that passed through an end-to-end TAG-certified channel – a supply chain in which the buyer, buy-side platform and sell-side platform are all certified. Measurement vendors including DoubleVerify and Integral Ad Science (IAS) were used to measure the rate of fraud in the sample, while IAS and Forensiq provided data on background fraud rates - the amount of fraud in the case where no fraud-prevention measures are taken.

The 614 Group research found an overall fraud rate of 0.53% within TAG-certified channels compared to a background level of 8.99%, indicating that implementation of TAG Certified Against Fraud decrease rates of invalid traffic by 94.1%.[234] However, the research methodology has limitations. Data provided by IAS, DoubleVerify and Forensiq is not independently verifiable; covers only invalid traffic, not other categories of ad fraud; and excludes any fraud that these vendors did not detect. In consequence, it is likely that the effectiveness of TAG certification is somewhat lower than the 614 Group data suggests.

7.4 JICWEBs Digital Trading Standards Group - brand safety

The JICWEBs Digital Trading Standards Group sets standards with the aim of reducing misplacement of digital advertising. These standards have a high level of adoption in the UK, though there is a lack of evidence of efficacy in reducing misplacement. The standards do not prevent the overreach of content-blocking that limits news publisher revenues.

7.4.1 Objectives

JICWEBS is the joint industry committee of the digital advertising industry made up for four trade bodies: the Institute of Practitioners in Advertising (IPA), the Incorporated Society of British Advertisers (ISBA), the Association of Online Publishers (AOP) and the Internet Advertising Bureau (IAB) UK. It oversees the development of good practice and standards for digital trading, and to increase transparency and trust in how digital advertising is bought and sold.[235] JICWEBS partners with its equivalent US organisation, The Trustworthy Accountability Group (TAG), which was founded five years ago to combat online ad fraud and piracy.

[234] 614 Group commissioned by TAG (January 2019). *TAG European Fraud Benchmark Study*.
[235] https://jicwebs.org/about-us/our-aim/

JICWEBS sets standards that companies can be independently verified against. In the field of brand safety, JICWEBs set up the Digital Trading Standards Group (DTSG) in 2012 with the aim of significantly reducing the risk of misplacement of advertising across the digital trading ecosystem.

7.4.2 Description

The DTSG standards involve forming appropriate contracts between buyers and sellers, using content verification tools, and setting out processes and policies for minimising ad misplacement and for takedown. These standards leave it to the buyer to define what content is unsafe for their brand. The specific good practice principles include:[236]

1. The Buyers and Sellers of digital display and audio advertising shall ensure that the transaction follows a Primary Agreement or Contract.

2. This contract should include where the advertising should (or should not) appear. The buyers and seller should use, independently-certified content verification tools[237] or schedules to minimise ad misplacement.

3. Sellers should confirm how they minimise the risk of ad misplacement, whether inventory is sourced directly or indirectly.

4. Sellers should be able to explain the process(es) that do this.

5. They should have policies defined, to respond appropriately to ad misplacement via takedown, and processes to meet these policies.

6. They should nominate a Responsible Officer for JICWEBS DTSG Brand Safety issues.

7. Each Signatory will have their ad misplacement minimisation policies independently verified by a JICWEBS-approved provider.

Certification is done by a JICWEBS-approved verification provider and is recertified annually. The verification provider reviews written information such as contract terms, a statement of reasonable endeavours applied to minimise the risk of ad misplacement, and internal policies, procedures and controls relating to the placement of ads.

7.4.3 Adoption

119 companies have been certified for the DTSG brand safety standards. All of the main agency groups (buyers) except Dentsu Aegis, several major publishers (sellers) and Facebook, Instagram, Google and Twitter are all certified. The breakdown of certified companies by category is set out in Figure 7.5. Industry stakeholders believe that take up of the standard is high due to the importance that advertisers are placing on brand safety.

[236] DTSG (June 2019). *UK Good Practice Principles for the Trading of Digital Display and/or Audio Advertising*.
[237] DTSG defines a content verification tool as a technology product or service that may block or report the serving of a display advertisement or the streaming or playback of an audio advertisement onto destinations that have been defined as inappropriate to the advertising campaign by the buyer.

Figure 7.5: Breakdown of DTSG brand safety certified companies by category, March 2020

Category of company	Number
Agency	23
Agency Platform Technology	1
Agency Technology	1
Platform	7
Platform Publisher Reseller Technology	1
Platform Technology	3
Publisher	26
Publisher Reseller	4
Publisher Technology	1
Reseller	7
Reseller Technology	20
Technology	25

Source: JICWEBS[238]

7.4.4 Efficacy

As we understand it, JICWEBS has not conducted research into the efficacy of DTSG brand safety standards. It may be challenging to quantify the impact of the standards, given that advertisers have different brand safety requirements and tolerances.

7.5 EDAA AdChoices

The European Interactive Digital Advertising Alliance's (EDAA) AdChoices is self-regulatory initiative aimed at fostering transparency in the online advertising environment, through delivering consumer-facing information on how data is used for online behavioural advertising and targeting. AdChoices is widely adopted in open display advertising but not social. In implementing the AdChoices logo, some companies also incorporate mechanisms for the reporting of ads and consumer control features. Although it is a consumer facing initiative, AdChoices do not directly address the consumer issues covered in Section 3.1.

7.5.1 Objectives

The European Interactive Digital Advertising Alliance (EDAA) is responsible for the 'AdChoices Icon' initiative targeted at companies active in digital advertising in Europe. The initiative is based upon IAB Europe's OBA Framework and EASA's BPR on OBA.[239] The overall objective of the AdChoices Icon is to increase consumer and marketer trust in interest-based advertising by linking through to consumer-friendly information about interest-based and online advertising.

[238] https://jicwebs.org/certification-process/signatories/ accessed 20 March 2020
[239] https://www.easa-alliance.org/sites/default/files/EASA%20Best%20Practice%20Recommendation%20on%20Online%20Behavioural%20Advertising_0.pdf

The AdChoices Icon initiative is developed with and for the online advertising industry and is intended to be an industry-wide, future proof and technology-neutral self-regulatory programme.[240] The objectives are two-fold:

1. to address growing concerns around consumer privacy and the consumer's online experience; and

2. to provide advertisers with a solution to rebuild consumer trust through enhanced transparency and control.

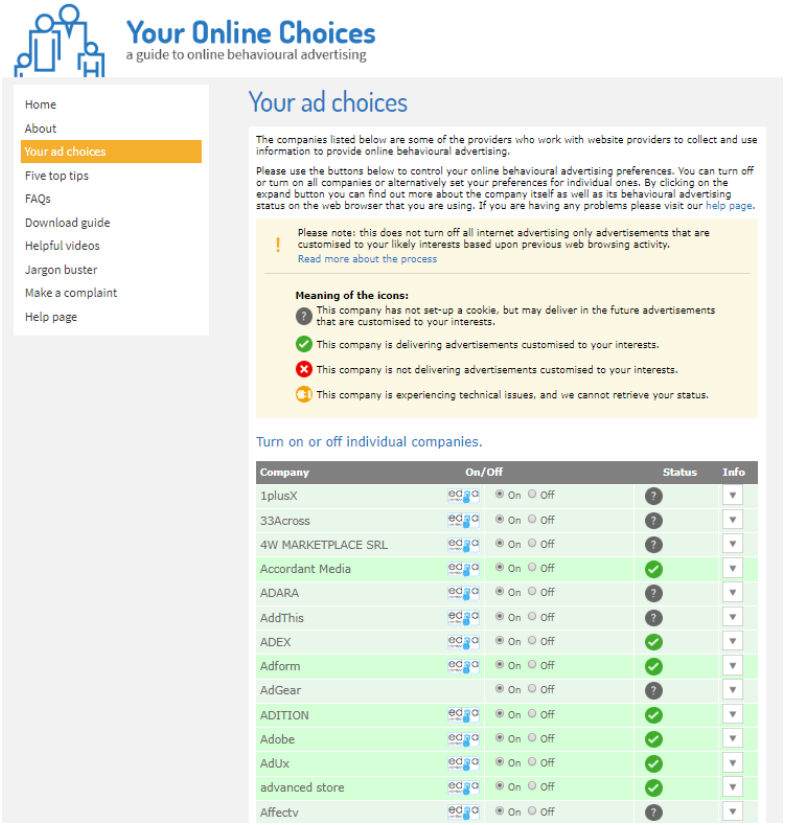
For consumers, the EDAA mission is to offer European citizens greater transparency, choice, and control over their online advertising and privacy preferences and provides easy-access information about how data-driven advertising works in practice.

For businesses, the AdChoices Icon is a self-regulatory programme which provides companies involved in online behavioural advertising (OBA) – website operators or third-party entities involved in OBA[241] – a means to provide enhanced notice of OBA practices to consumers. The programme is designed to enable to complement existing legislation and other industry self-regulatory initiatives, whilst ensuring that the online advertising industry continues to help Europe's digital sector thrive and innovate.

The EDAA also runs a Consumer Choice Platform for consumers and companies *YourOnlineChoices.eu* which provides tips, guidelines and FAQs relating to the AdChoices Icon initiative, as well as more general information on behavioural advertising and online privacy. The platform also allows consumers to control their online advertising preferences by turning off the third-party entities involved in online behavioural tracking as shown in Figure 7.6. As of end 2019, 111 companies were active on the Consumer Choice Platform.

[240] The technical specifications for the AdChoices Icon initiative are developed by IAB Europe and the European Advertising Standards Alliance (EASA).
[241] These companies engage in the displaying of ads on unaffiliated websites, using own or acquired Data-Driven Advertising data in the process, and in the collection of data online for advertising, or use data to deliver ads.

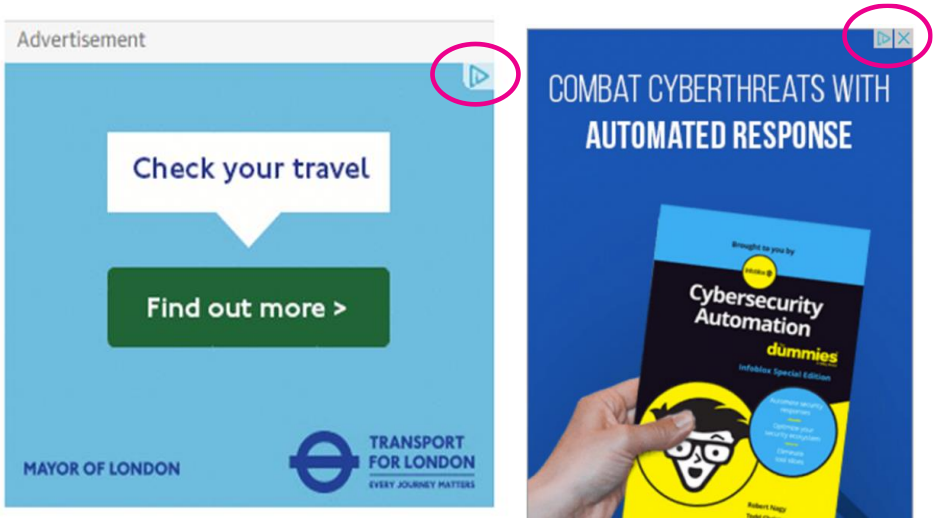
Figure 7.6: EDAA Consumer Choice Platform



7.5.2 Description of initiative

The AdChoices Icon is a consumer-facing, interactive tool, symbolising consumer transparency, choice and control over interest-based advertising. It is an interactive symbol to be placed in or around online ads (by "Third Parties"), or on websites where OBA data may be collected and/or used (by "Website Operators"). Figure 7.7 provides an illustration of the AdChoices Icon.

Figure 7.7: AdChoices Icon



For companies, there is a three-step process certification process:

1. Apply to start using the AdChoices Icon – the application form and technical guidelines are provided via the EDAA website.[242] The annual fees range from zero (website operators with purely national focus or readership) to €3,000 (SME) to €5,000 (non-SME).[243]

2. Integrate with the Consumer Choice Platform in the case of third-party entities.

3. Comply with the European self-regulatory principles for OBA – this involves:

   - Self-certification within 6 months of starting to use the AdChoices Icon or being integrated on the Consumer Choice Platform.[244]

   - Independent certification within 7 months – all "Third Parties" must independently verify their compliance with an approved Certification Provider. Certification Providers will grant successful companies a renewable Trust Seal, owned by EDAA, which will act as a representation to the market and to consumers that the company is fully compliant with the Self-Regulatory Programme.

Following the certification, companies are also subject to regular compliance checks on their policies and guidelines.

For consumers, the Icon is intended to provide real time information on an ad in a simple and transparent manner which is not available through other tools such as the browser. Figure 7.8 and Figure 7.9 illustrate the reporting and feedback options available to consumers when clicking the Icon on ads served by Google. It should be noted that the implementation of the AdChoices interstitial or landing page differs by vendor and in many cases, there are fewer options and less information available to consumers than that provided by Google.

[242] http://www.edaa.eu/what-we-do/for-companies/
[243] https://www.edaa.eu/fees/
[244] http://www.edaa.eu/self-certify/

Figure 7.8: Google ad network (options upon closing the ad)

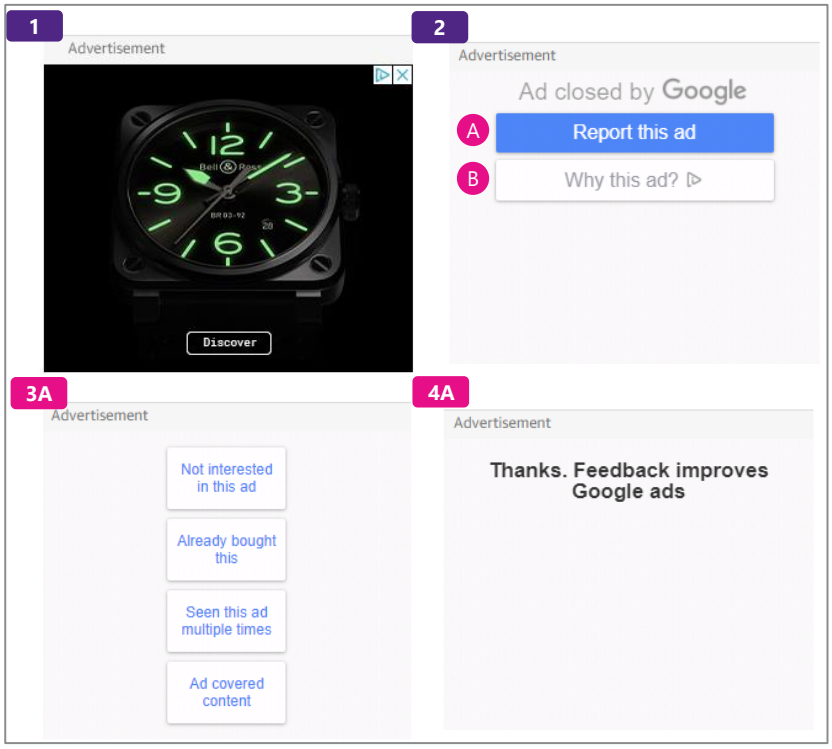
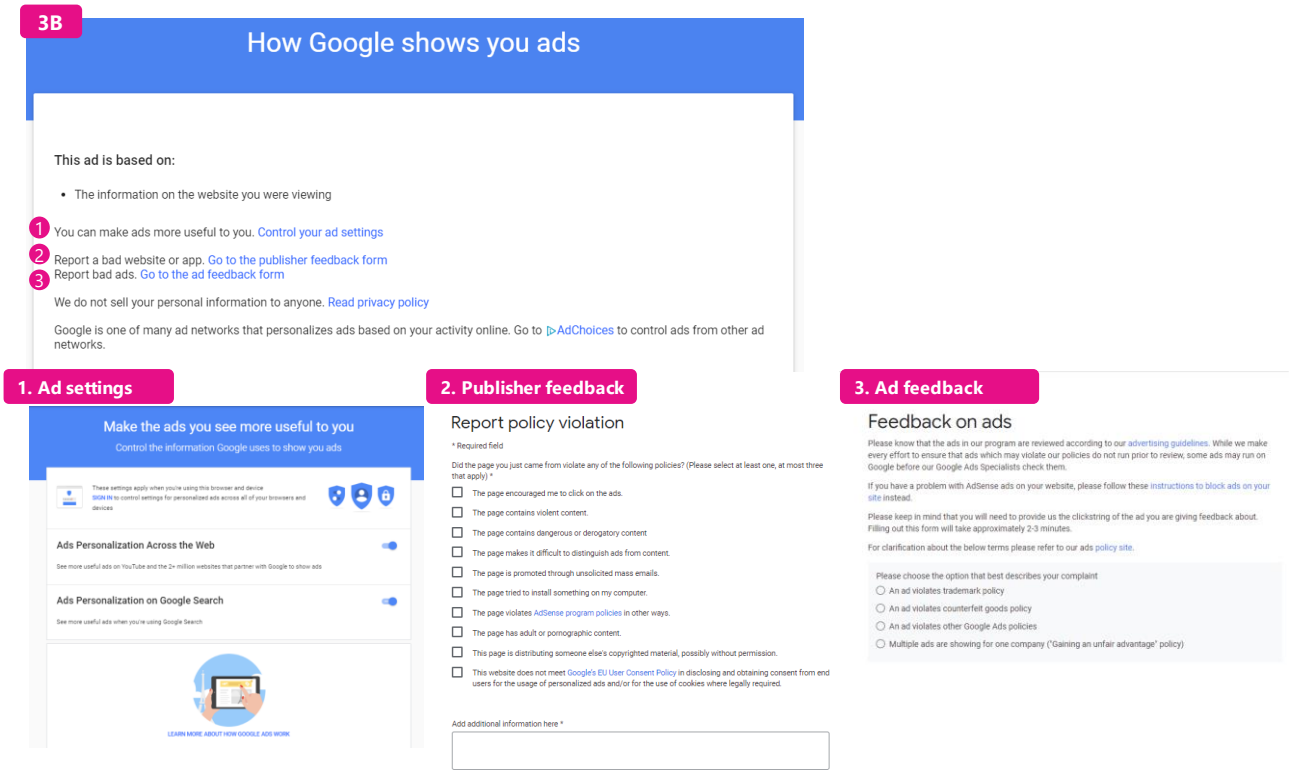


Figure 7.9: Google ad network (information and options upon clicking on the AdChoices Icon)



7.5.3 Adoption

As of December 2019, 155 companies were participating in the EDAA Self-Regulatory Programme on Data-Driven Advertising. The majority of these companies are involved in the delivery of online open display advertising. In 2019, over 162 billion Icons were delivered on online ads across Europe, through a combination of the approved Icon Providers, Evidon, Crownpeak and TrustArc.[245] It is estimated by the EDAA that these participating companies are responsible for more than 90% of the open online display ads delivered in the UK.[246]

However, there are some notable exceptions. For example, ads served on Facebook[247] and YouTube do not display the AdChoices Icon although links to AdChoices and the Consumer Choice Platform are available on both Facebook and YouTube.[248]

7.5.4 Efficacy

While the vast majority of online display ads do display the AdChoices Icon, evidence on consumer interaction with the Icon is limited. A 2019 EDAA survey of consumers in five European countries (France, Germany, Poland, Spain and the UK) found that one in three consumers have used the Icon.[249] The survey also indicated that users of the AdChoices Icon tend to feel more informed, have a better understanding of data use, and are more receptive towards OBA and site personalisation, compared to those who have not used the Icon or the Consumer Choice Platform.

However, we were not able to obtain further information on:

- the proportion of ad impressions on which the Icon was clicked by consumers,
- the reasons why consumers had clicked on the Icon – to find out why the ad was being served or to lodge a complaint, and
- the subsequent actions taken by consumers, how the complaints were addressed or taken into account by the ad networks, and any redress provided.

Such information, if made available by the ad tech vendors, such as Google, would have provided an indication on the volume of ads which raised consumer concerns, the nature of these concerns (e.g. inappropriate content or targeting) and extent of these issues.

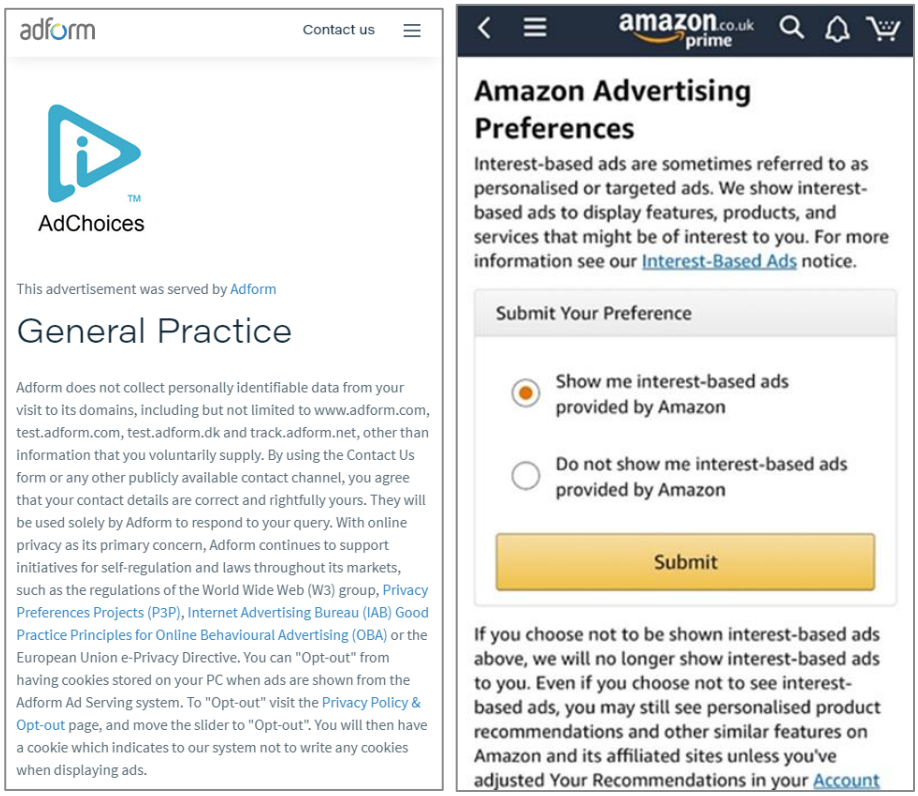
A potential issue from the consumer perspective is the lack of consistency in the options and information available to consumers after clicking on the Icon. These vary by ad tech vendors and there are over 100 ad networks who are certified under the programme. The Google example illustrated above provides various reporting options and details for consumers. Other ad tech vendors tend to provide less information and more basic options, as illustrated in Figure 7.10.

The EDAA policy sets the basic technical specifications for the AdChoices Icon and requires participating companies to provide a link through to the Consumer Choice Platform. Aside from these, companies are given the flexibility to adapt the interstitial page and include additional options and information they provide to consumers. This reduces the cost of compliance for smaller ad tech vendors but also allows participating

[245] EDAA (2019). Activity Report. https://www.edaa.eu/wp-content/uploads/EDAA-Activity-Report-2019.pdf
[246] Industry estimates.
[247] With the exception of Facebook Audience Network – an advertising network which allows advertisers to extend their Facebook and Instagram campaigns to other mobile apps or platforms.
[248] For example, on clicking on the 'Why this ad?' logo on YouTube sends a user to Google's ads setting page where a link to AdChoices is provided.
[249] https://www.edaa.eu/consumer-research-how-eu-citizens-perceive-digital-advertising-since-gdpr/

companies to take extra steps to be more transparent. However, the resulting differences in the level of information and options available could impede consumer awareness and understanding.

Figure 7.10: AdChoices Icon – options on Adform and Amazon ad networks



7.5.5 Incentives/Barriers to adoption

In terms of incentives for adoption by industry, successful companies are granted a renewable Trust Seal, owned by EDAA, which will act as a representation to the market and to consumers that the company is fully compliant with the Self-Regulatory Programme. The trading seal is envisaged to have a significant market value to compliant businesses, conveying a sense of trust and good standing from consumers and business partners towards the company that receives it.

The AdChoices Icon is a voluntary initiative and meeting the compliance standards is a resource-intensive process. The flexibility in EDAA's policy on the implementation of the AdChoices Icon helps with adoption as smaller third-party companies may otherwise find it difficult and costly to comply and implement comprehensive reporting and feedback systems.

7.5.6 Future developments

For the next iteration of the AdChoices Icon programme, the EDAA is looking to improve the mechanisms for data exchange and communication among different levels of the supply chain. The objective is to address challenges of the fragmented supply chain in the open online display advertising ecosystem and to improve transparency and accountability.

8 Platform rules and policies

8.1 Platform advertising policy scope

Platforms and open display advertising intermediaries have advertising policies governing advertising content and practices. These policies are generally referenced in the terms and conditions of advertiser contracts. Under these terms, platforms generally have the right to cancel ads and suspend or terminate the accounts of advertisers in breach of policies. Generally, under platform terms, advertisers are also required to comply with relevant law and regulations. Facebook Self-Serve Ad Terms require that 'Your ads must comply with all applicable laws, regulations and guidelines, as well as our Advertising Policies.'[250]

Some platform advertiser policies go beyond the advertising codes in prohibiting or restricting certain advertising, such as spyware, malware and hacking content. Figure 8.1 lists the areas covered by Facebook and Google advertising policies in the UK. Other platforms and intermediaries also have advertising policies, such as Snapchat,[251] Twitter,[252] LinkedIn,[253] and Xandr.[254] Platforms are constantly evolving their policies as new trends or issues emerge. For example, Google announced a new advertiser identity verification programme in April 2020 which will require advertisers to submit their legal business or individual name for verification.[255] This will feed into a new ad disclosure initiative that will display an advertiser's name and country. For open online display ads this information will be available via the AdChoices icon.

Figure 8.1: Overview of Facebook and Google's advertising policies

Policy areas	Facebook	Google
Prohibited content	• Community Standards • Illegal products or services • Discriminatory practices • Tobacco and related products • Drugs and drug-related products • Unsafe supplements • Weapons, ammunition or explosives • Adult products or services • Adult content • Third-party infringement • Sensational content • Personal attributes • Misinformation • Controversial content • Non-functional landing page • Cheating and deceitful practices • Grammar and profanity • Non-existent functionality • Personal health • Payday loans, payslip advances and bail bonds • Multi-level marketing • Penny auctions	• Counterfeit Goods • Dangerous products or services – Explosives – Guns, gun parts & related products – Other weapons – Recreational drugs – Tobacco • Enabling dishonest behaviour – Hacking software or instructions – Services designed to artificially inflate ad or website traffic – Fake documents – Academic cheating services • Inappropriate content – Dangerous or derogatory content – Shocking content – Sensitive events – Animal cruelty • Ads & Made for Kids Content – Violent and Graphic Content – Scary Imagery – Crude Humour – Profanity and Sexual Innuendo

[250] https://en-gb.facebook.com/legal/self_service_ads_terms
[251] https://www.snap.com/en-GB/ad-policies
[252] https://business.twitter.com/en/help/ads-policies.html
[253] https://www.linkedin.com/legal/ads-policy
[254] https://wiki.xandr.com/display/policies/Policies+for+Buying
[255] https://www.blog.google/products/ads/advertiser-identity-verification-for-transparency/

Policy areas	Facebook	Google
	• Misleading claims • Low-quality or disruptive content • Spyware or malware • Automatic animation • Unacceptable business practices • Circumventing systems • Prohibited financial products and services • Sale of body parts	– Significant Skin Exposure
Restricted content	• Alcohol • Dating • Real money gambling • Regional lotteries • Online pharmacies • Promotion of over-the-counter medicines • Subscription services • Financial and insurance products and services • Branded content • Ads about social issues, elections or politics • Disclaimers for ads about social issues, elections or politics • Cryptocurrency products and services • Drug and alcohol addiction treatment • Cosmetic procedures and weight loss	• Adult Content • Alcohol • Copyrights • Gambling and games • Healthcare and medicines • Political content • Financial services • Trademarks • Legal requirements • Other restricted businesses • Restricted ad formats and features • Ads & Made for Kids Content (restrictions on a wide range of ad categories on Made for Kids content)
Rules on advertising practices	• Targeting (must not use targeting options to discriminate against, harass, provoke or disparage users, or to engage in predatory advertising practices) • Positioning (Relevance, Accuracy, Related landing pages) • Data use restrictions • Text in ad images	• Abusing the ad network • Data collection and use • Misrepresentation • Editorial standards • Destination requirements • Technical requirements • Ad format requirements
Review process	• Checks include advert's images, text, targeting and positioning, and content on advert's landing page. • Most ads are reviewed within 24 hours	• All content in ad is reviewed, including headline, description, keywords, destination and any images and video. • Most ads are reviewed within one working day.

Note: Google also has similar policies for YouTube content creators wishing to monetise their content and certain criteria must be met before creators are allowed to run advertising.[256]
Source: Facebook[257], Google[258]

In addition to their advertising policies, Facebook and Google have developed measures to prevent specific forms of harmful advertising. Facebook requires advertisers in certain categories to certify compliance with its non-discrimination policy[259] which discourages discriminatory targeting. Facebook has also removed certain targeting options that might be used in a discriminatory way.[260]

[256] https://support.google.com/youtube/answer/6162278?hl=en-GB
[257] https://www.facebook.com/policies/ads
[258] https://support.google.com/adspolicy/answer/6008942?visit_id=637250354143995815-931308344&rd=1
[259] https://www.facebook.com/business/help/338925176776440
[260] https://www.facebook.com/business/news/keeping-advertising-safe-and-civi l

Google has certification programmes that require advertisers in certain categories to meet conditions before their ads are approved to run. These programmes are in place for categories that are sensitive or prone to abuse, such as gambling,[261] secondary ticketing[262] and debt services[263] advertising.

8.2 Policy enforcement

The effectiveness of platform policies in preventing harmful advertising depends on advertiser awareness of these policies and platform enforcement. We do not have information about levels of advertiser awareness. In terms of enforcement, Facebook and Google use machine and human review to screen ads, and they act on reports of any inappropriate ads not stopped by these screens.

These platforms are applying advanced technologies, such as artificial intelligence, to identify inappropriate ads. They can draw on strong research and engineering skills and resource to support this activity. Facebook has a global team of 35,000 staff working on safety and security. Facebook reviews each new ad before it goes live based on an analysis of its component parts – by machine, with human input when required. If an ad is disapproved, then an advertiser may edit the ad or appeal. Facebook also reviews live ads if these are reported to it or flagged up by its AI system and stops running ads found to violate Facebook's policies. Facebook reviews about 10 million ads per month in the UK and approves about 95% of these.[264]

Facebook and Google do not provide detailed information about the methods used to detect certain categories of inappropriate advertising or the effectiveness of these methods, due to security sensitivities. Our view is that platform ad screening is likely to be relatively more effective at identifying obviously harmful content, such as advertising for weapons, than content where a subjective judgement is needed or the harmful nature of the advertising is concealed by sophisticated bad actors such as in some cases of malicious advertising. And it is unlikely that platform screens will identify ads that make misleading claims, as validation of advertiser claims requires bespoke research.

[261] https://support.google.com/adspolicy/answer/6018017?hl=en#apply
[262] https://support.google.com/adspolicy/answer/7577050?hl=en&ref_topic=1316596
[263] https://support.google.com/adspolicy/answer/9520029
[264] Source: Facebook

9 Technology solutions

9.1 Cybersecurity solutions

Technology plays an important role in combating malware, ad fraud and brand safety risk, as well as identifying instances of inappropriate advertising. In many cases, major owned and operated platforms have developed proprietary technology solutions, while participants in the open display advertising market tend to use solutions from third-party vendors. The efficacy of these solutions is generally very difficult to determine, given that these vendors report the amount of malicious advertising or ad fraud that these services detect, but not the undetected quantity.

9.1.1 Third-party anti-malware solutions

There are four main cybersecurity vendors who help online open display advertising supply chain participants screen ad impressions for malicious advertising: Ad Lightning, Confiant, Risk IQ and The Media Trust. The detailed approaches used by these vendors is not well documented due to security considerations and commercial confidentiality. Generally, they develop intelligence about malware threats, identify these threats in ad creative and block ads. Confiant is differentiated by conducting checks on ad creative on user browsers.

We do not have data about the uptake of these services by supply chain participants. Ad Lightning, Risk IQ and The Media Trust have the TAG Certified Against Malware seal and are likely to be used to scan a subset of the three-quarters of UK online open display advertising impressions that are covered by this TAG programme (see Section 7.2.3).

9.1.2 Fraud and brand safety verification services

Ad verification providers offer independent analytics services that identify whether ad impressions are brand safe, viewable and non-fraudulent traffic – in other words, whether the ads were served in reputable content and seen by real people as intended. Generally, verification providers place tags on ads which collect data and report this back to their servers. The providers use analytics on this data to identify and flag:

- Potentially fraudulent ad impressions, such as impressions resulting from bot fraud.
- Non-viewable ad impressions, such as ads served on parts of a web page the user does not scroll down to.
- Non-brand safe ad impressions, such as ads served against illegal, harmful or offensive content.

Generally, this process is conducted after ad impressions have been served. In some cases, ad verification providers also provide "pre-bid" analytics which predict the likelihood of ad impressions being non-valid (non-viewable, non-brand safe or fraudulent). Market participants use this information to inform bidding decisions.

The main ad verification and anti-fraud providers are Integral Ad Science (IAS), Oracle, Double Verify, White Ops, Forensic, Cheq and Anura. There is limited data about the methodologies used by these providers. The effectiveness of their services is also difficult to determine:

- Efficacy in reducing ad fraud. Some vendors report rates of fraudulent traffic in the case that traffic is optimised using their services. IAS reported worldwide ad fraud rates of 9.5% of total ad impressions in

H1 2019, which fell to 1.1% after optimisation using IAS services, indicating that optimisation prevents the sale of 88% of fraudulent impressions.[265] However, this data is not independently verified and will exclude any fraud that goes undetected by IAS.

- Efficacy in improving brand safety. IAS reported UK rates of brand risk in pages screened ranging from 2.8% in desktop display to 9.8% in desktop video.[266] Advertisers using IAS services would be able to filter out these pages. However, there is no independent verification data about what proportion of risky content this technology identifies – or how much is flagged up as a false positive.

9.1.3 Proprietary solutions

Major platforms have generally developed their own, proprietary solutions to prevent inappropriate advertising and, in the case of Google, ad fraud.[267] There is very limited information about these solutions, given security sensitivities around these activities.

In the case of inappropriate advertising, platforms are applying advanced technologies, such as artificial intelligence, to identify inappropriate ads. For example, as discussed in Section 8.2 above, Facebook's ad review process is based on an analysis of its component parts – by machine, with human input when required.

In relation to ad fraud, Google uses live reviewers, automatic filters, machine learning, and deep research to block as much invalid and fraudulent activity as possible.[268] A global team of over a hundred PhDs, data scientists, engineers and researchers monitors and analyses traffic for invalid clicks, impressions, views, or interactions, and stops publishers generating invalid activity from receiving undeserved advertising income. Google's automated detection systems use machine learning and complex algorithms. It manually reviews suspected cases of invalid activity that were not stopped by its automated systems. When it finds unusual traffic, or an advertiser or publisher raises a valid concern, Google's team investigates the data and makes a decision or creates a new filter.

9.2 Distributed ledger technology

Distributed ledger technology is currently being trialled in the UK and has the potential to create a closed online display advertising ecosystem in which ad fraud and malicious advertising would be more difficult.

9.2.1 Objectives

Distributed ledger technology (DLT),[269] is a way of digitally recording transactions across a distributed (peer-to-peer) network of computers so that any involved record cannot be altered retroactively. In the online display advertising market, JICWEBs set up a DLT pilot in the UK, working with technology vendor Fiducia. The purpose of the DLT is to evaluate how DLT technology could bring greater accountability to digital advertising transactions and address trust, transparency and inefficiency problems. This technology also has potential to increase standards compliance within the supply chain.

[265] IAS (2019). *Media Quality Report H1 2019*.
[266] IAS (2019). *Media Quality Report H1 2019*.
[267] Ad fraud occurs mainly in the open online display advertising market. Google acts as an intermediary in this market. Other owned and operated platforms such as Facebook, Instagram, Twitter and Snapchat, play a more limited role.
[268] https://www.google.com/ads/adtrafficquality/
[269] Blockchain is one form of distributed ledger technology.

9.2.2 Description

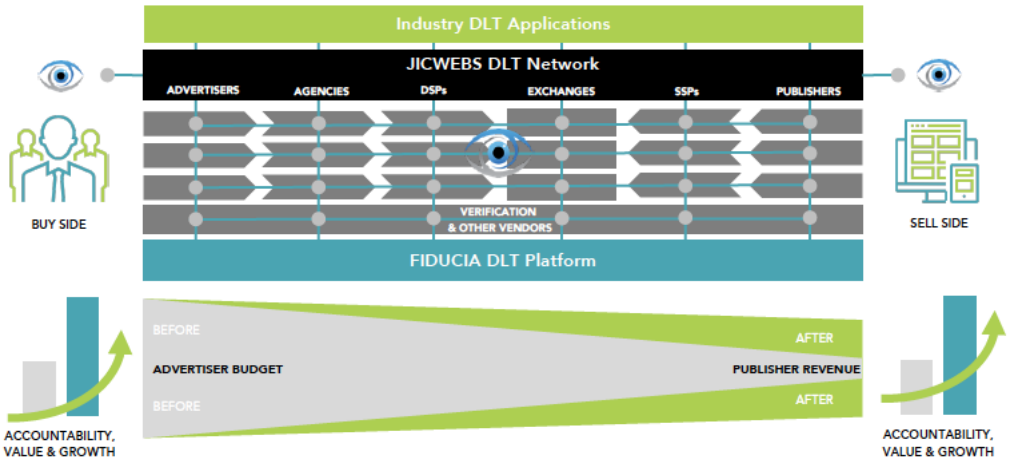
The DLT pilot, running from July 2019 to March 2020, involves a consortium of market participants including major brands, agencies, ad tech vendors and publishers, representing different parts of the online advertising supply chain, including:

- Advertisers: Unilever, Nestlé, McDonald's, Virgin Media, Telefonica, Johnson & Johnson, National Theatre
- Media agencies: WPP, Publicis, Omnicom, IPG, Havas, Altair
- Ad tech vendors: Xandr, Rubicon, Integral Ad Science, Moat/Oracle
- Publishers: Sky, eBay, Gumtree, Rightmove, Netmums

Figure 9.1 illustrates the structure of the DLT platform and its interaction with participants. Pilot participants – the JICWEBS DLT Network - connect to the Fiducia DLT platform through nodes (devices on the peer-to-peer network). They write agreed data fields to the ledger, such as information about ad impressions. This data forms an immutable record of transactions and events. The data is encrypted and can be decrypted by other participants if smart contracts (replicating legal contracts) between organisations allow this – for example, to facilitate audits or reconciliation of transactions.

The DLT network is permission based. Participants need to register and comply with terms and conditions set by JICWEBS. This feature allows JICWEBS to regulate who joins the network and under what terms. The pilot is evaluating how DLT can enforce "live compliance" with regulation, industry standards, certifications and best practices. The DLT platform allows ongoing monitoring of measurable requirements of network participants.

Figure 9.1: Fiducia DLT network and platform



Source: Fiducia

JIWEBS and Fiducia have completed the pilot and an independent evaluation committee is assessing how the pilot met its objectives and considering questions about selection of technology partner and of governance. It now hopes to move on to develop a minimum viable ecosystem (MVE), a larger-scale implementation of the DLT network involving a broader industry consortium and a potential market launch in 2021.

9.2.3 Efficacy

JICWEBS and Fiducia claim benefits for pilot participants included business risk reduction due to stronger compliance and reduced fraud, cost reduction and optimisation of the supply chain. In relation to the issues addressed in this study, DLT – if adopted widely - has the potential to:

- Limit ad fraud and malicious advertising by creating a closed, permission-based online open display advertising ecosystem. Regulation of market access through registration would prevent direct participation by bad actors.
- Regulate the adoption of standards. JICWEBS could impose requirements to adopt and comply with self-regulatory standards relating to brand safety, fraud and malvertising – as terms of entry to the network. The DLT could also be used to support monitoring of compliance against these standards.
- Reduce ad fraud by enabling easier reconciliation of data between participants and the identification of fraudulent ad impressions.

9.2.4 Drivers and barriers to adoption

The DLT network would need to involve a critical mass of industry participants in order to have a significant impact. The benefits of DLT may incentivise some market participants to join. JICWEBS and Fiducia report that participants in the pilot are keen to develop DLT to the next stage. However, the DLT pilot is a UK initiative in a global market. Most advertising technology intermediaries and vendors operate globally and might not wish to take a different approach in the UK to other markets, unless they expect this approach to become global. Achieving industry alignment on rules and requirements for the network could also be a challenge. JICWEBS would need large numbers of stakeholders to agree on a common approach.

10 Consumer awareness campaigns

10.1 AA 'Media Smart' campaign

Media Smart is an industry-led education campaign funded by the Advertising Association (AA). It aims to improve media literacy among children and teenagers in the UK through the provision of media and digital literacy resources for teachers, parents and youth organisations. While the initiative provides young people with a better understanding of online advertising and the critical skills to evaluate such ads, it does not directly address the specific consumer issues in scope.

10.1.1 Objectives

Media Smart is an advertising industry-led consumer awareness campaign from the Advertising Association that provides educational resources for 7 to 16-year olds to help develop the understanding and tools to be "critical consumers of media".[270] It includes resources on social media, digital advertising, body image, and influencer marketing. Media Smart's provides resources for teachers and parents, primarily through topic guides and Media Smart's blog (for example parental guide to gaming).[271] One of Media Smart's key objectives is to maintain a neutral stance on advertising, meaning that it does not advocate advertising of any kind to be 'good' or 'bad'.

Media Smart was initially launched in 2002 and was re-established in 2014 with a greater focus on the role of digital advertising and social media. The broad mission of the campaign is to equip children from a young age with the skills required to critically navigate the media and advertising that they consume. Media literacy is a key objective and relevant to several of the Advertising Associations' policy areas.[272] The Advertising Association posits that the digital resilience skills that the Media Smart campaign aims to provide with regards to digital advertising and social media are transferable to other media issues, such as fake news. Furthermore, the Advertising Agency note that the campaign aims to address gaps in the current ICT curriculum that currently focuses on the use of technology rather than critical skills regarding ICT and content consumed.

Media Smart is supported by advertisers, agencies, media and trade bodies and the Advertising Association has indicated that industry support is growing. In 2019-20, Media Smart received annual funding from 13 industry supporters and has recently increased its number of strategic partnerships, which often offer resources or ad credit in lieu of funding.

10.1.2 Description of initiative

Media Smart's website provides educational resources for teachers and parents, that are targeted at different age groups. Media Smart's social media feeds aim to predominantly promote the campaign and resources to teachers and schools. Current resources for teachers are summarised in Figure 10.1.

[270] https://mediasmart.uk.com/about-us/
[271] https://mediasmart.uk.com/gaming/parents-guide-to-gaming/
[272] Confirmed to Plum by Advertising Association representatives in stakeholder / research meeting.

Figure 10.1: Media Smart teaching resources[273] (February 2020)

Primary school resources	Secondary school resources
• An Introduction to Advertising – 7-11 years, key stage 2&3 • Digital Advertising PSHE accredited teach resource – 9-11 years, key stage 2 & 3 • Body Image & Advertising resource – 9-11 years, key stage 2 & 3	• Body Image & Advertising – 11-14 years, key stage 3 • Social Media resource – 11-16 years, key stage 3 • Influencer Marketing resource – 11-14 years, key stage 3

The teachers' resources on each topic include teachers notes on the subject matter, along with presentation and/or video resources, and student worksheets. The resources aim to encourage students to critically assess commercial influence on digital advertising and content, and to evaluate digital products (for example to evaluate different types of social media available or to identify influencer marketing as a form of advertising) amongst other topics.

The Media Smart website also includes several publicly available top-line guides aimed at parents and guardians. These include:

- Body Image & Advertising – 9-14 years. The guide aims to provide an introduction on body image and advertising, to support positive body image in young people.

- Digital Advertising & Social Media – 9-11 years. This parent guide was developed with the support of academics and industry experts and aims to explain the presence of advertising in social media and how it functions (for example, the techniques used to gain consumer attention).

In addition to this, Media Smart's blog offers additional articles and resources examining issues related to social media, gaming, digital advertising, media literacy, and providing links to other useful educational resources.

Media Smart's resources and wider syllabus has been developed with input from numerous stakeholders. The topic areas are informed by the policy and consumer research undertaken by advertising industry think tank CREDOS and the media literacy research undertaken by Ofcom. The resources are developed by educational consultancy EdComs and reviewed by subject matter experts and the ASA or other relevant regulatory bodies. Media Smart also receive input from the PSHE Association which helps develop and accredit the resources and further promotes the resources to PSHE teachers. The resources are periodically reviewed and updated to ensure they remain accurate; for example, the educational resources covering social media have been reviewed to ensure recent entrants to the social media market are included.

The Media Smart campaign is further promoted on The Times educational resources website and First News, a weekly newspaper aimed at children and circulated in schools.[274] It also uses ad credit (often supplied from strategic partners) to target teachers and parents as well as relying on word-of-mouth among teachers to promote the campaign.

10.1.3 Adoption

Media Smart reports approximately 63,000 downloads of its teaching resources – of these, 20% were by parent/guardians/youth leaders; 55% by primary school teachers and 25% by secondary school teachers.[275]

[273] Primary school teaching resources: https://mediasmart.uk.com/primary-resources/, Secondary school resources: https://mediasmart.uk.com/secondary-resources/
[274] Further information on First News: https://www.firstnews.co.uk/
[275] Source: Advertising Association.

It is difficult to assess the Media Smart campaign's overall adoption or impact given the lack of evaluation of the initiative due to budget constraints.

10.1.4 Efficacy

The Media Smart campaign does not directly address the consumer online advertising issues in scope of this study (inappropriate advertising or targeting – as set out in Section 2.2). Media Smart report anecdotal evidence that teachers have commented on students having increased awareness of advertising and more indication to critically assess media following use of Media Smart teaching resources. The feedback received by Media Smart from teachers and students has been considered when developing resources, but Media Smart noted that they are unable to acquire in-depth feedback due to budget. Therefore, there is limited evidence on the adoption and impact of the campaign.

To the extent that the Media Smart campaign helps to increase awareness and knowledge of the mechanics of online advertising, this may help increase usage of relevant consumer tools which are available to address some of the potential harms associated with online advertising (see Section 8 for more information on consumer tools and services).

10.1.5 Future developments

Media Smart are currently working with EDAA in order to develop resources on the issue of use of data and personal privacy.

There is also an appetite to undertake further surveying and research to understand the campaign's impact and areas for development. In particular, there is interest to extend the Media Smart programme to younger children under 7 years old if budget was made available to undertake this work.

The Advertising Association also noted the opportunities beyond the scope of the Media Scope campaign. This included furthering adult media literacy and for vulnerable groups in particular. For example, improving media literacy to support financially vulnerable individuals from gambling and payday loans ads.

The Advertising Association also indicated that they would welcome more support from the Government and public bodies (such as DCMS, Department for Education and Ofcom) to help promote and extend the Media Smart campaign in terms of both its visibility and awareness, and resources available.

10.2 ICO 'Be Data Aware' campaign

The *Be Data Aware* campaign by the Information Commissioner's Office (ICO) aims to educate consumers on how and why personal data is used for targeting purposes in online advertising, social media and political campaigning. The campaign, which has been run primarily on social media, does not directly address the specific issues in the scope of this study. The reach of the campaign was less than 0.1% of the UK's online population.

10.2.1 Objectives

The *Be Data Aware*[276] campaign is part of a broader consumer data awareness strategy by the ICO referred to as *Your Data Matters*.[277] The motivation behind the campaign was the ICO's investigation into the use of data analytics in political campaigns[278] and the aim is to help consumers understand how their personal data is being used and why.

The ICO have created a number of resources aimed to explain how companies might be using personal data to target consumers online and why, and how consumers can control who they are being targeted by. The initiative focuses on four main areas:

- Social media privacy settings
- Microtargeting
- Political campaigning practices – direct marketing
- Political campaigning practices – data analytics

The ICO *Be Data Aware* campaign page includes a video that explains how targeted advertising works, using previous Internet search history to then offer adverts for similar products or services (the campaign example uses search and targeted advertising for holidays). The campaign video goes on to explain that "companies collect and share information from many different sources and use it to predict what people like [the consumer] are interested in. They make tailored adverts to match these interests…" It then explains that online political campaigns also use the same techniques in order to personalise their campaign message to individuals in order to influence their vote. It should be noted that the scope of the *Be Data Aware* campaign is broader than digital advertising or data collected from online platforms.

Be Data Aware was run mainly a social media campaign[279] with an animation and website resources (including press release) as collateral. The campaign was launched in May 2019 ahead of the European Parliament election and was publicised on the ICO website blog[280] and in national and industry press.

10.2.2 Description of initiative

The ICO provides specific information for consumers on the four campaign areas, which were identified following its investigation into the use of data analytics in political campaigns.[281] The four areas are summarised in the subsections below. The information provided focuses on data privacy and targeting; the campaign does not directly address issues relating to online advertising such as fraudulent, misleading and harmful advertising or misplacement of advertising.

10.2.2.1 Social media privacy settings

The ICO provide an extensive summary on social media privacy and advises that individuals should check the privacy and advertising settings before using a social media (or other) service and to review these settings

[276] See: https://ico.org.uk/your-data-matters/be-data-aware/
[277] See ICO's Your Data Matters resources: https://ico.org.uk/your-data-matters/
[278] ICO (July 2018). Democracy disrupted? Personal information and political influence. Available at https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[279] This was run across the @ICOnews and @YourDataMatters social media handles.
[280] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/helping-people-be-data-aware/
[281] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

regularly.[282] ICO also provides factsheets to help guide individuals change their advertising and data privacy settings on a range of social media platforms, including Facebook, Twitter, Snapchat, LinkedIn, and Google.[283] The guidance on the web page further encourages individuals to check privacy settings from a desktop in addition to the mobile operating system as there may be some visual differences in how the information is presented in a mobile app. It encourages individuals to contact the providers of the social media platform if they have further queries on how to adjust their privacy settings or advertising preferences.

The ICO information also notes the 2017-2018 investigation into use of personal data, and the subsequent investigation into data collected by a third-party app on Facebook that was shared with Cambridge Analytica. There is specific guidance on what individuals should do if Facebook has informed them that their data was captured and shared.

10.2.2.2 Microtargeting

The ICO information on microtargeting provides a brief overview to explain what microtargeting is, how it works and explains how consumers can limit microtargeting on social media alongside simple contextual examples to aid consumer understanding.[284] It should be noted that the information refers to microtargeting predominantly from social media rather than microtargeting from wider digital platforms (for example, from browsers and search engines) though the information presented to consumers is somewhat transferable.

The ICO describes microtargeting as "a form of online targeted advertising that analyses personal data to identify the interests of a specific audience or individual in order to influence their actions… used to offer a personalised message to an individual or audience". It notes that advertisers and individuals will benefit from more relevant and personalised ads being displayed.

It further explains that microtargeting works through electronic tracking tools, such as Cookies, Social Plug-ins and Tracking Pixels, that collect information on the users' browsing habits and social media likes to build a profile about the user. The profile information is then used to provide individually tailored adverts, and that this may also be shared with third parties operating on social media.

The ICO information encourages users to review social media providers' "Settings" or "Account Settings" to limit microtargeting.

10.2.2.3 Political campaigning practices – direct marketing

There is fairly extensive information provided on direct marketing for political campaigning.[285] The ICO reiterates that campaigners and candidates must act within the law, especially in how and when individuals are contacted and how personal information is collected and held. It notes that political parties and candidates are entitled to receive a copy of the full electoral register and that the electoral register is often used in conjunction with information acquired about the individual online.

The ICO information outlines the methods that political campaigns can use to contact individuals and the consent requirements. These include via post personally addressed to the individual and phone calls (unless the individual has opted-out or objected to this kind of marketing), and via email, text, fax and automated phones if

[282] ICO web page on social media privacy settings, associated with Be Data Aware: https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/
[283] ICO factsheet on Facebook social media privacy settings (example): https://ico.org.uk/media/your-data-matters/documents/2614882/ydm-facebook-factsheet.pdf
[284] ICO web page on microtargeting, associated with Be Data Aware: https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/
[285] ICO web page on political campaigning practices: direct marketing, associated with the Be Data Aware campaign: https://ico.org.uk/your-data-matters/be-data-aware/political-campaigning-practices-direct-marketing/

the individual has opted-in and provided their consent. The information provided further outlines rules around political campaign market research, use of contact details collected from constituency casework, and continued use of data following a change in the elected representative's political party membership.

The ICO provides guidance to help individuals evaluate whether an organisation is right (allowed) to collect and use their personal data and it outlines potential actions that the individual can take to raise a concern and/or stop receiving marketing from organisations and political parties.

10.2.2.4 Political campaigning practices – data analytics

The ICO referenced its investigation which found political parties and campaigners had used microtargeting or "data analytics methods" to target potential voters. Information was provided on whether the use of data analytics for political campaigning is allowed, the ICO's role in regulating this, and action that concerned individuals may take to protect their data and themselves from political microtargeting.[286]

It also highlighted the ICO's actions, based on the 2018 report about the investigation and findings of data analytics used by political parties and campaigners. With respect to advertising, the ICO notes that: "Online platforms who provide advertising services to political parties and campaigns should have expertise within the sales support team who can provide advice on transparency and accountability in relation to how data is used to target users" and that a statutory Code of Practice regarding use of personal data in political campaigns should be introduced.

The ICO information further recommends the following actions for individuals to protect their personal data.

- Individuals should be aware of how and why they are seeing certain messages online – i.e. understanding the role of data analytics and targeted advertising.
- Individuals should be aware of rights under data protection law.
- Individuals should consider changing their social media privacy settings – this refers to ICO's Be Data Aware web page on social media privacy settings (discussed above).
- Individuals should keep up to date with ICO advice and guidance – ICO links to their social media accounts or to sign up to the ICO monthly newsletter.

10.2.3 Efficacy

The campaign was run by the ICO twice in 2019, during May 2019 and December 2019 ahead of the UK General Election. The campaign was promoted primarily through social media and some media outlets. Its impact in terms of reach is in the "tens of thousands" [287] which represents less than 0.1% of the UK's online population.

In terms of addressing specific consumer issues in online advertising, the efficacy of the campaign is somewhat limited, particularly as the campaign focus is more on privacy and political campaign aspects. However, to the extent that the campaign has helped raise awareness of the privacy tools on social media platforms (see Section 8 below) and the mechanics of online behavioural targeting, the campaign has contributed to general media literacy and could nudge consumers towards making more informed decisions in relation to online advertising.

[286] ICO web page on political campaigning practices: data analytics, associated with the Be Data Aware campaign: https://ico.org.uk/your-data-matters/be-data-aware/political-campaigning-practices-data-analytics/
[287] Plum interview with ICO, March 2020.

10.2.4 Future developments

Information on the Be Data Aware campaign remains on the ICO's website. However, there are no immediate plans by ICO to relaunch the campaign.

11 Consumer tools and services

This section provides an overview of the controls available to consumers that enable some choice over the type of adverts they will see when using the internet. It covers the advertising and service settings of major online platforms – Facebook and Google – as well as browser controls and ad blocker tools.

11.1 Ad settings on Facebook

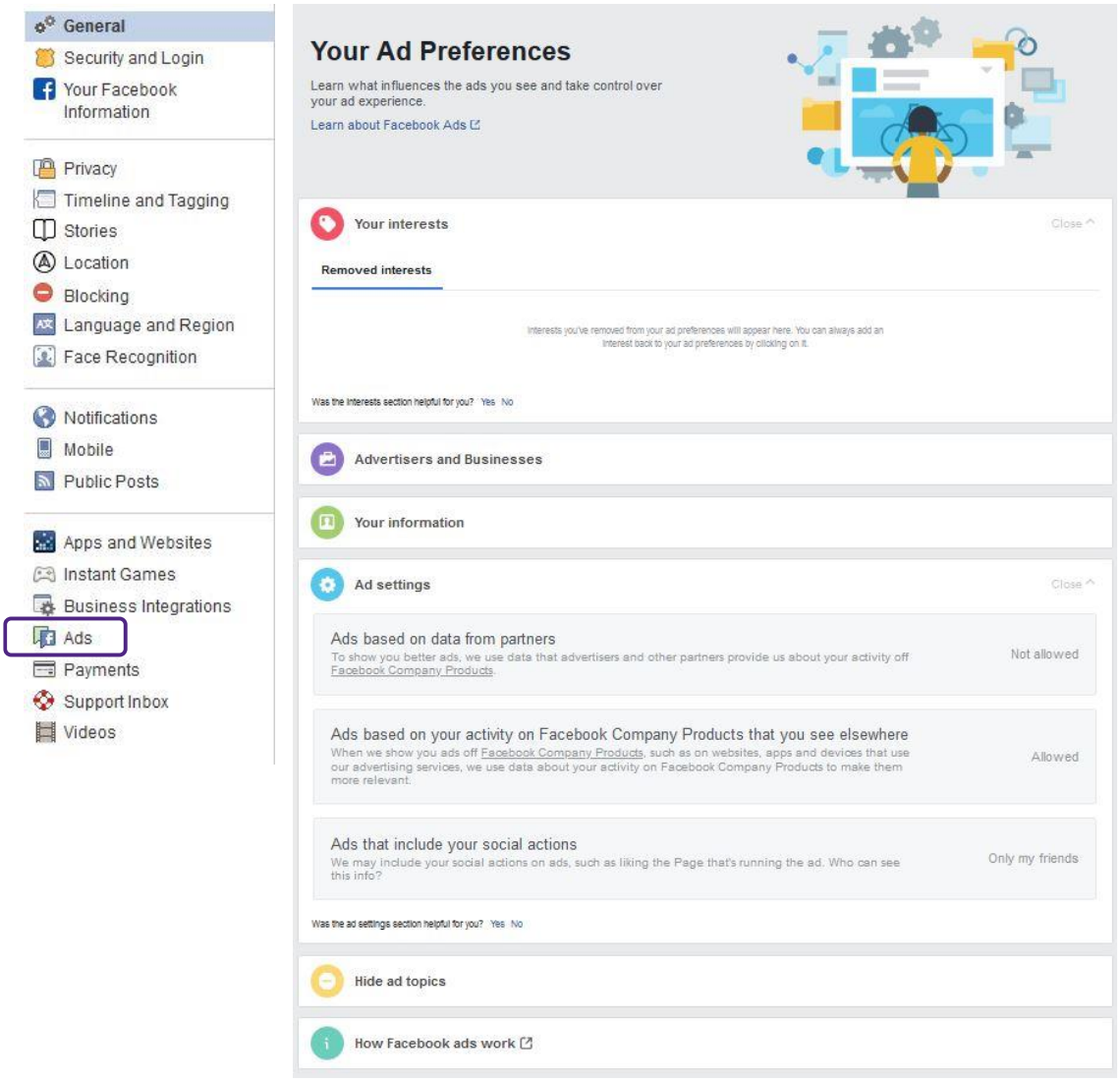
Facebook ad settings allow users a level of control over how personal data is used for delivering targeted ads and also a choice to hide certain advertising topics. These settings could help mitigate some of the consumer issues set out in Section 3.1 such as inappropriate targeting and misleading ads for some ad topics, on Facebook and Facebook Audience Network. However, there is limited evidence to assess their effectiveness.

11.1.1 Objectives

Facebook ad settings are meant to provide its users with more control over how data is used to determine what ads are served and to provide more information on why users are seeing a particular ad.[288] The objective is to improve transparency over ad targeting and allow users to customise their preferences to see ads that are more relevant and/or acceptable to them through the ad preference settings shown in Figure 11.1.

[288] https://www.facebook.com/ads/about/?entry_product=ad_preferences

Figure 11.1: Facebook ad settings



11.1.2 Description

Facebook's ad settings enable Facebook users to review and manage their personal information, interests and customise their ad preferences.[289] Users can change the following ad settings:

- **To allow or not allow ads based on data from Facebook partners, such as browsing history or purchasing on partner websites and apps:** This setting applies to ads seen on Facebook, Messenger, as well as websites, apps and devices that use Facebook's advertising services.

- **To allow or not allow Facebook Audience Network to use data gathered on Facebook and its other products for the targeting of ads on third-party apps or websites:** The guidelines mention that if the user does not allow Facebook's ad preferences, the user "will still see ads, but they won't be as relevant" to the user and that the user "may still see ads for other reasons such as age, gender, location, the content in the app or website used, [the user's] activity outside the Facebook Companies."

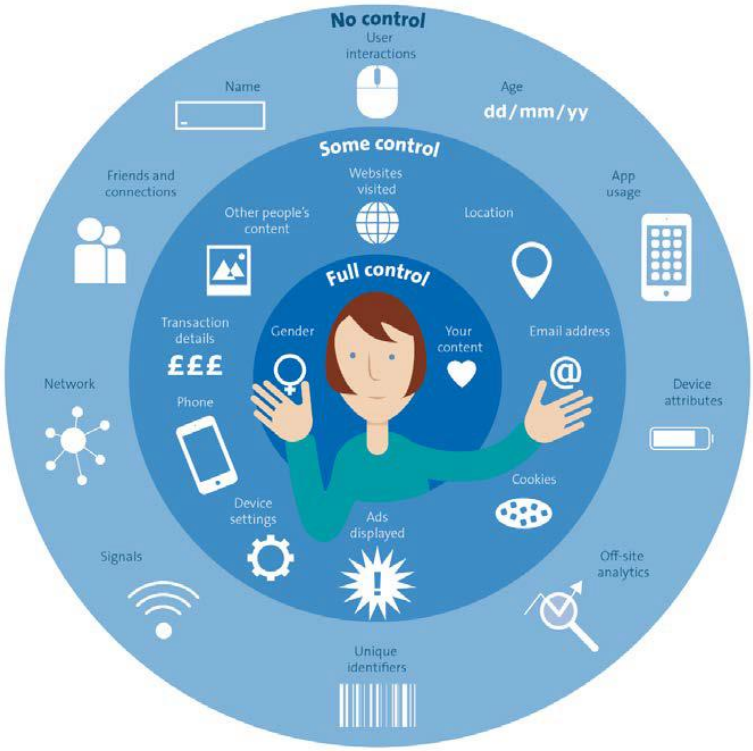
[289] https://www.facebook.com/ads/preferences/?entry_product=education_page

- **To allow or not allow ads that include the user's social actions:** Facebook friends of a user (except users under 18) will see ads based on actions taken by the user (events joined, your likes, follows, comments, shares, app usage, check-ins and recommendations), if they have permission to view the actions taken by the user. The user can choose whether his/her personal "Likes' are displayed in adverts.

In the ad settings, the user can also hide some ad topics (alcohol, pets, parenting, any suggested sensitive topic chosen by the user) for a duration of 6 months, 1 year or permanently; and see why he/she is seeing a particular ad. In the default settings, the user's activity is used for personalisation of ads that are issued by Facebook on other websites, but users do not see ads of Facebook's partners based on their Facebook activity.

It is notable that these settings allow users to restrict use of Facebook data for targeting off Facebook, and off-Facebook data for targeting on Facebook, but users have little control over use of Facebook data for targeting on Facebook itself; user control is only limited to social actions. Figure 11.2 illustrates the levels of user control over data collected and used for ad targeting.

Figure 11.2: Illustrative levels of control over information collected by Facebook



Source: CMA[290]

11.1.3 Adoption

Facebook does not publish data on consumer usage of these ad preference tools.

[290] CMA (December 2019). *Online platforms and digital advertising. Market study interim report*, Appendix F.

11.1.4 Efficacy

The availability of these settings may also help mitigate some of the potential issues relating to inappropriate targeting, such as discrimination and vulnerable audiences,[291] but it is not possible to assess the efficacy of these settings in addressing such concerns as information on usage of these tools are not available.

The ability for users to hide some ad topics such as alcohol, parenting and pets, may, to an extent, help to mitigate potential issues relating to offensive or harmful ads and ads for some sensitive category, illegal or restricted products and services. However, the purpose of this Facebook setting is to let people block ads to avoid stirring painful memories, rather than to specifically address online advertising issues. Facebook noted that these were the typical categories which users report to be distressing or upsetting.[292] There are no figures on the number of users who make use of these settings.

Furthermore, the need for consumers to take proactive steps to adjust these settings suggests that efficacy would differ by individual consumers and this will depend on how well-versed users are with the tools available to them and also on general level of media literacy.

11.1.5 Drivers and barriers to adoption

For consumers, once they are able to locate the relevant page,[293] the information given and the user guidelines are quite self-explanatory. However, there are also potential barriers to adoption, including:

- Lack of awareness or incentives: Making changes to ad settings requires proactive action by the user.
- Accessibility: Ad settings are not easily accessible. By clicking on "Settings", the user gets access to a list of 20 types of settings (see Figure 11.1), including general, security and login, privacy, location, blocking, etc. "Ad settings" is the 17th on the list. This is confirmed in CMA's report: "Facebook's settings web page can only be reached via a menu whose location is not prominently displayed on the Facebook website".[294]

Educating consumers on these settings can help to empower users and drive adoption.

11.2 Ad settings on Google

Google ad settings offers users the choice to limit personalised advertising served by Google. These settings are designed to address privacy concerns and to improve transparency around the use of data for advertising, and do not have direct impact on the consumer issues in scope.

11.2.1 Objectives

Google uses personal data of its users to offer them personalised ads in Google products, on partners' websites and in mobile applications. In its policy on ads and data, Google states:

[291] Note that Facebook also has a separate non-discriminatory policy for advertisers which is intended to address some of these issues.
[292] https://adage.com/article/digital/facebook-lets-users-block-ads-stir-painful-memories/307193
[293] https://www.facebook.com/ads/about/?entry_product=ad_preferences
[294] CMA (December 2019). *Online platforms and digital advertising*. Appendix F, p.F37.

> **"While these ads help fund our services and make them free for everyone, your personal information is not for sale."**
>
> **"We give advertisers data about their ads' performance, but we do so without revealing any of your personal information. At every point in the process of showing you ads, we keep your personal information protected and private."**[295]

Google allows users to adjust ad settings for its owned and operated services (YouTube, Maps etc) and third-party properties it serves ads into as listed in Figure 11.5. In its privacy and safety principles, Google states that

> **"Each user has different expectations regarding data confidentiality. This is why we offer privacy settings in Google accounts that everyone can choose to activate or not activate according to their needs. And as technology evolves, so do our privacy settings, to ensure the user can always make their choices freely."**[296]

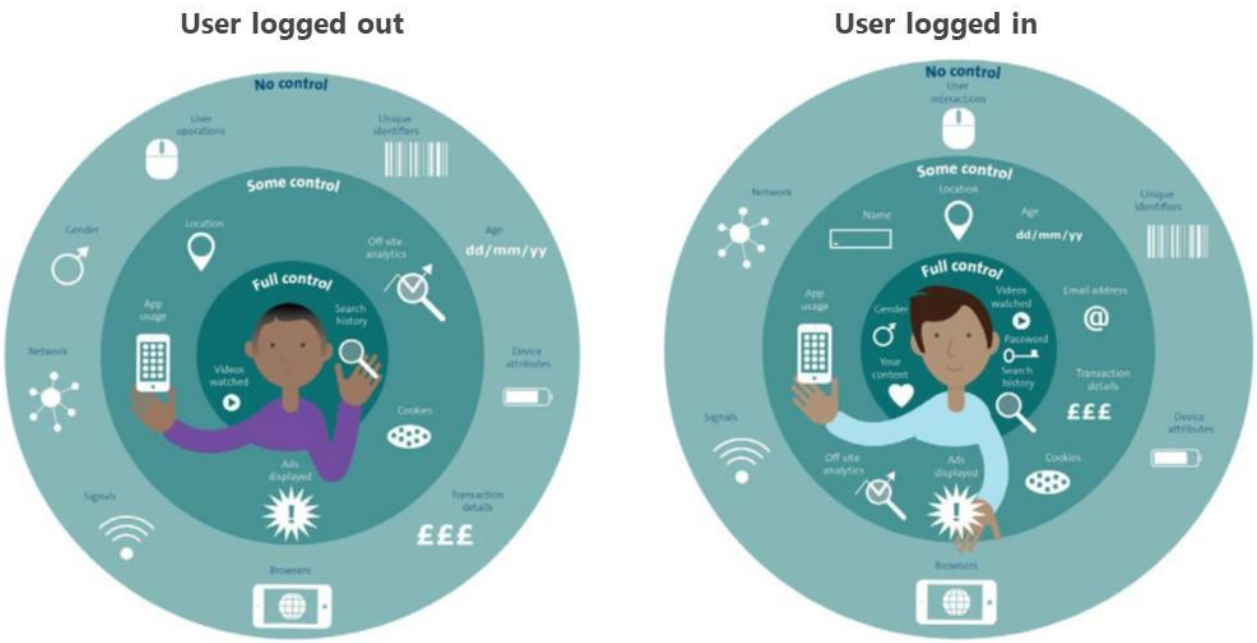
Note that besides using the ad settings provided by Google, ads served by Google on third-party websites and apps also adhere to the AdChoices Icon initiative (this is discussed separately in Section 7.5).

11.2.2 Description

Google enables users to create an account in order to get access to various services (calendar, email, file storage) whilst not being mandatory to use the search functionality. Account settings provide tools for users to control certain ad settings. Data used includes the searches done by the user, their location, websites and application usage history, videos and ads seen, as well as information like age range and gender. Such data then informs the ads seen by the user, depending on the user's ad settings and if they are signed in or not. The CMA has found that "being logged-in gives consumers more control over how their data is used, compared to consumers who are not logged-in" as illustrated in Figure 11.3. [297]

[295] https://safety.google/privacy/ads-and-data/
[296] https://safety.google/principles/
[297] https://safety.google/principles/

Figure 11.3: Illustrative levels of control over information collected by Google



Source: CMA

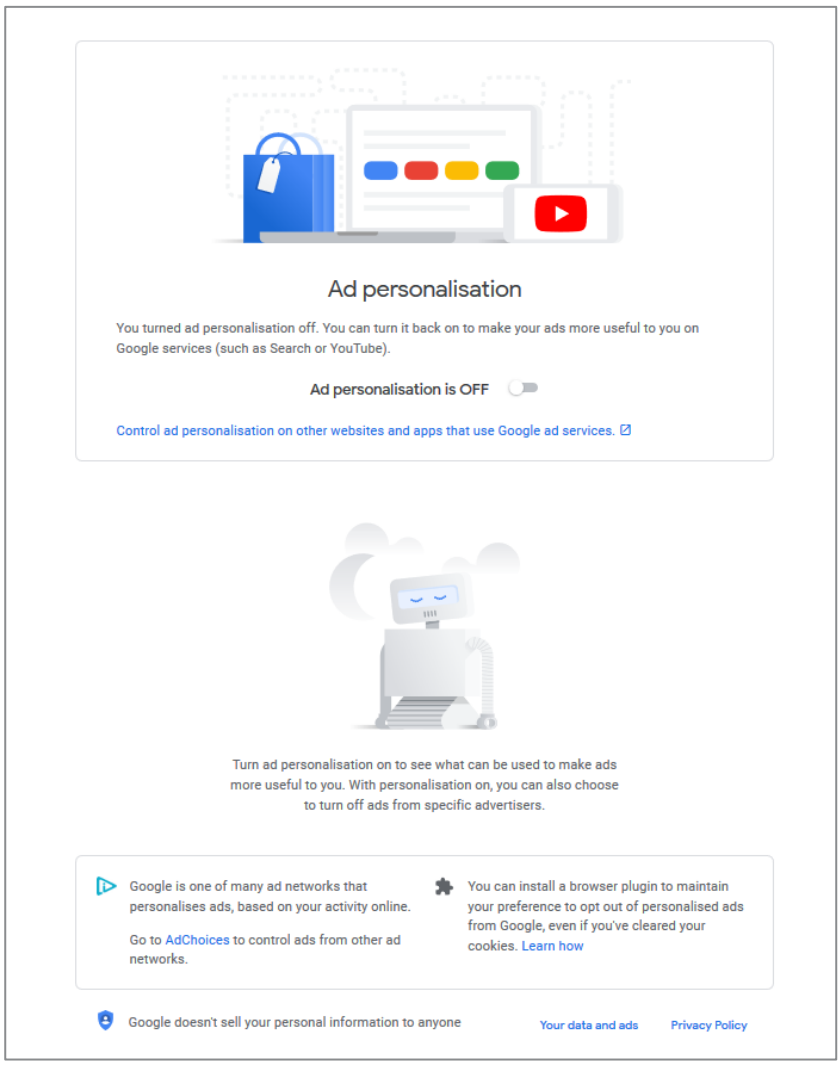
Google settings does not enable the user to block all ads, but to receive personalised ads and to block certain ads. Possible controls and settings are described below.

11.2.2.1 Personalised ad settings

Every Google user account has its own ad settings. If the user has signed in with two different Google accounts, the ad settings will be those of the default account (the account that was signed in with first). The user can personalise their ad settings by clicking "ad personalization is ON" (note this is the default setting) and choose the websites and apps that use Google ad services that they want to receive personalise ads from.

It is also possible to stop getting ads that are based on personal interests and information by choosing "ad personalisation is OFF" on the Ad personalisation page (Figure 11.4). In this case, the user will continue to receive ads, but these will be less targeted; instead, Google ads will use information like general location, or the content of the websites visited.

Figure 11.4: Steps to turn off personalised ads on Google

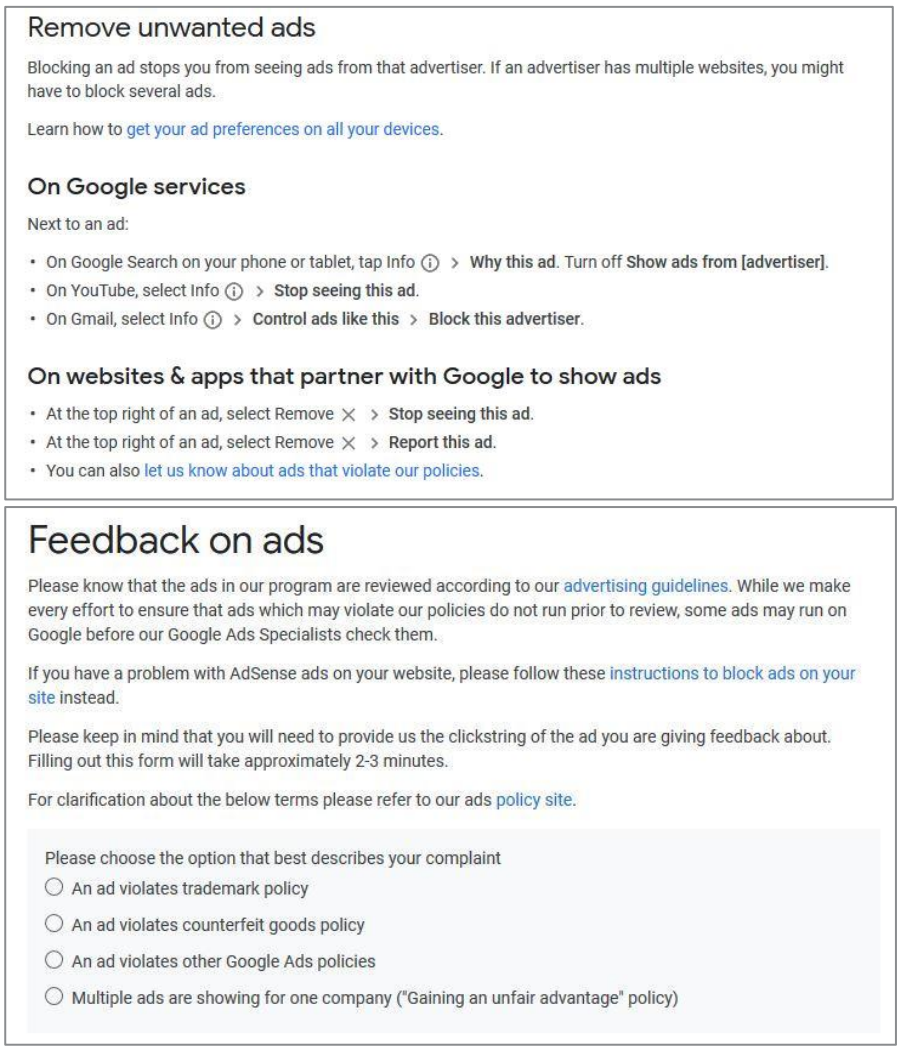


Source: Google

11.2.2.2 Blocking unwanted ads

Blocking an ad will apply to all ads from the advertiser (Figure 11.5). This needs to be done on multiple ads if the advertiser has multiple websites. This can be done on Google Search, YouTube, Gmail, as well as websites and apps that are Google partners. (For more details on the process involved, see Section 5.5.2)

Figure 11.5: Steps to block unwanted ads



Source: Google

11.2.3 Adoption

Google does not publish data on adoption rate or usage of these ad settings by consumers.

11.2.4 Efficacy

With regard to ad personalisation, the ad settings are designed to provide transparency and clarity on data use in the delivery of customised ads through data-driven targeting techniques, and also to provide a greater degree of control to users. In this respect they are effective in addressing the stated objectives. However, they do not directly address specific consumer issues identified in Section 2.2.

To the extent that a user receives more relevant ads, they may be less likely to receive certain ads which could be perceived as offensive or harmful. Conversely, a user who opts out of personalised ads may be more susceptible to inappropriate targeting, all things equal. It should be noted that there is an inevitable element of subjectivity involved in such issues as individual preferences will vary. There will also be potential trade-offs in terms of data privacy which is beyond the scope of this study. It is not possible to assess these aspects without

information on the adoption of these settings and outcomes for users. Such an exercise will require significant further study.

With regard to ad blocking settings, these provide users with a mechanism for reporting and blocking unwanted ads. This could help individuals alleviate potential issues of fraudulent, misleading and harmful advertising, and mis-targeting of advertising. At a broader level, ad blocking settings may be less effective in addressing issues around discriminatory targeting or targeting of vulnerable audiences.

11.2.5 Drivers and barriers to adoption

The use of ad personalisation settings requires proactive steps to be taken by consumers. This could be a potential barrier if there is insufficient incentive for them to do so. It should be noted that incentives could be driven more by concerns over data and privacy issues, instead of online advertising harms. Greater user awareness of these tools and education initiatives (see Section 7) could help address the awareness barrier and equip users with the appropriate information to make their own decisions on whether to use these settings.

The use of ad blocking requires a series of steps to be taken by the user as outlined in Figure 11.5 which may not always be intuitive and may pose adoption barriers. In addition, the provision of feedback also requires some familiarity with Google Ads policies which may not be obvious to many users. Thus, unless the perceived harm to the individual is significant, there may be a lack of incentive for users to take the necessary steps to provide the feedback to Google.

11.3 Web browser ad controls

Web browser ad controls give users the ability to restrict or block cookies which are used by ad tech companies for ad targeting purposes. Providers of web browsers are increasingly looking to block third-party cookies which will limit personalised ad targeting, and thus reducing potential inappropriate targeting issues. Settings which help to block malware and redirects could also help to address some cases of malicious advertising.

11.3.1 Objectives

Most web browsers (Firefox, Safari, Edge, Internet Explorer, Google Chrome, etc) provide some form of privacy settings to restrict or block cookies from being stored on users' devices. These are designed to limit tracking by third-party cookies, block pop-up ads and malicious scripts. The objectives of these controls are to enhance privacy and to improve user experience on the web.

11.3.2 Description

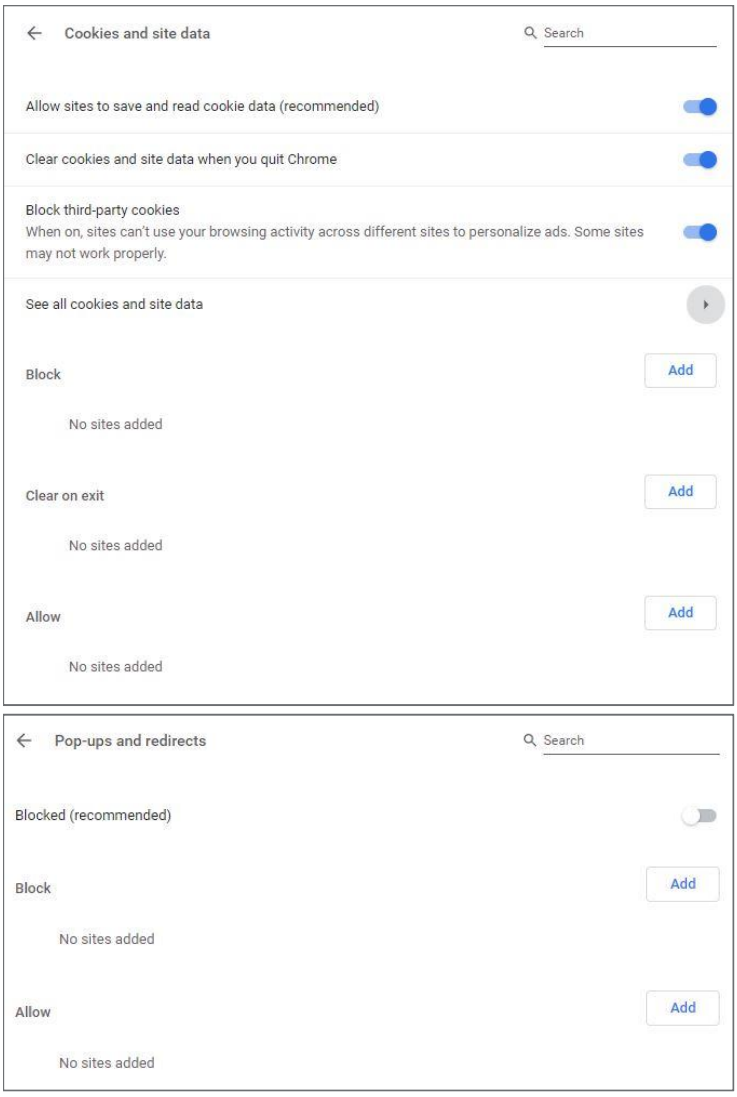
Third-party cookies are small text files which travel between a browser and the website of a company displaying ads on the page which a user visits.[298] Ad technology companies make use of these cookies to keep track of ads served and to help deliver relevant ads – by matching identifiers between companies. Third-party cookies also allow advertisers to control frequency (the number of times a user sees an ad) and to track the effectiveness of ad campaigns. Most browsers offer three cookie filtering settings: allow all cookies, block third-party cookies, or

[298] In contrast, first party cookies are created by the host domain and are generally considered helpful to users as they provide a better user experience and keep the session open.

block all cookies. Several leading browsers either already block third-party cookies by default (e.g. Firefox,[299] Safari[300]) or have announced plans to do so (Chromium[301]).

Separately since February 2018, Chrome has allowed its users to limit their exposure to pop-up ads, via their browser settings. This can be done by clicking "blocked" on "pop-ups and redirects". This setting blocks all ads on sites that repeatedly violate standards that have been set forth by the Coalition for Better Ads[302,303] (also see Section 7.1 on IAB Gold Standard). This includes full page ads, ads with auto play sound and video, as well as ads that appear with a countdown blocking the user before the content loads. Figure 11.6 shows the relevant cookie and pop-up settings on Chrome.

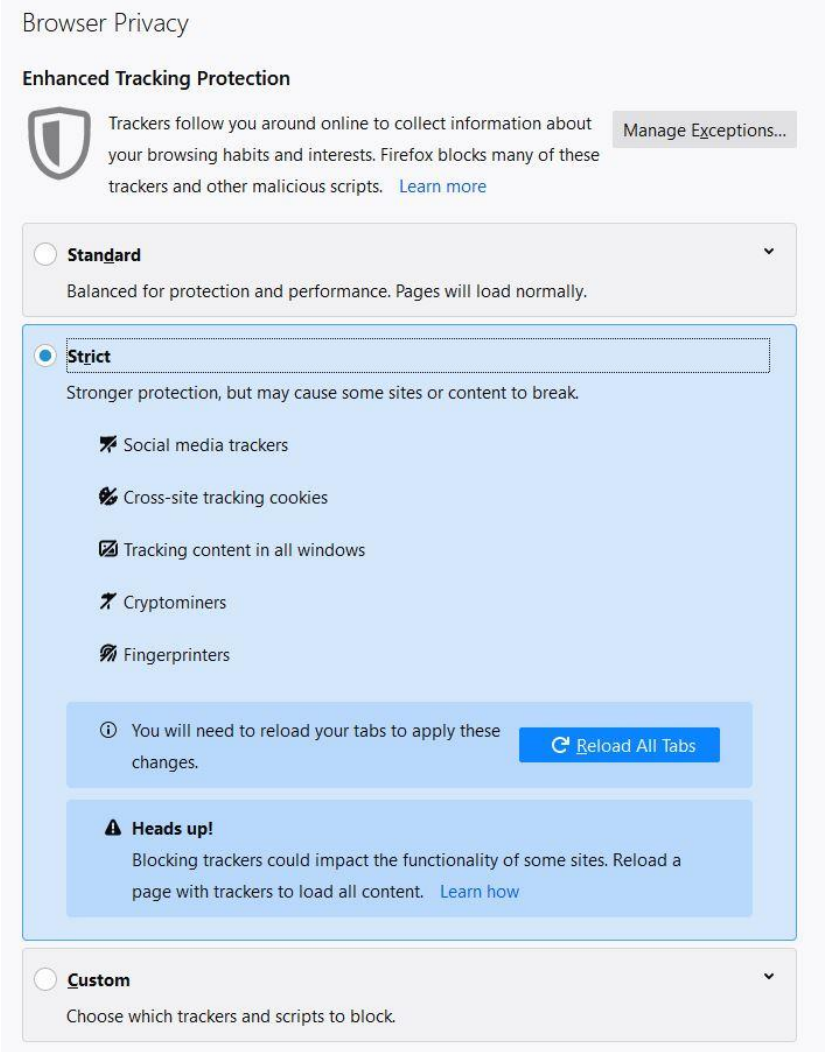
Figure 11.6: Chrome browser settings



[299] Mozilla announced in June 2019 that new users of the Firefox browser would have the 'Enhanced Tracking Protection' setting turned on by default and thus blocking known third-party tracking cookies. This was subsequently rolled out to all existing Firefox users in a later release in September 2019. For more information, see https://blog.mozilla.org/blog/2019/06/04/firefox-now-available-with-enhanced-tracking-protection-by-default/.
[300] In March 2020, Apple announced that the latest update to its Safari browser that all third-party cookies will be blocked by default for all users. For more information, see https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
[301] In January 2020, the Chromium Project announced its intention to phase out support for third-party cookies within two years while also working to address the needs of users, publishers and advertisers through a healthy, ad-supported online ecosystem. For more information, https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html
[302] Sites are warned before they are blocked.
[303] https://www.betterads.org/standards/

Like Chrome, Safari enables users to block pop-ups. In order to use external content blocker apps on Safari, the phone must have iOS9 or higher. This setting stands on iPhones in "Settings", then "Safari"; and on Macs in "Safari preferences", then "Security". In addition to blocking cookies and trackers, Firefox also provides protection against malicious scripts as illustrated in Figure 11.7.

Figure 11.7: Firefox browser protections



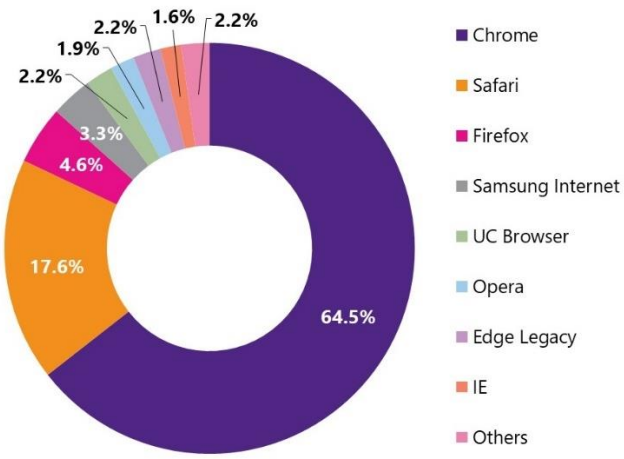
11.3.3 Adoption

There is limited publicly available information on the proportion of users who tailor their browser settings to enhance privacy and protection against malware. According to Mozilla, more than 20% of Firefox users have turned on its 'Enhanced Tracking Protection' feature prior to its recent move to implement this by default.[304]

Chrome dominates the market in terms of market shares as shown in Figure 11.8. At present, third-party cookies are not blocked on Chrome although this is set to change by 2022, which will mean that by then virtually all users will be blocking third-party cookies.

[304] https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

Figure 11.8: Market share of all browsers – global (February 2020)



Source: StatCounter

11.3.4 Efficacy

To some extent, the use of browser settings helps to curtail personalised advertising and enhance user privacy which is the objective of browser controls. In the case that the user browser limits personalised targeting by disabling third-party cookies, the user is less likely to be affected by inappropriate targeting done on the basis of their personal data. However, there remains a risk that they could be targeted inappropriately based on context or first-party data.

Browser settings may also enable users to reduce the risk of being exposed to malware in ads. However, cybersecurity experts interviewed for this project indicated that cyber criminals design malicious advertising to bypass these browser controls.

Lastly, it should be noted that these controls are only applicable to online activity through web browsers. Increasingly, consumer online activities are through mobile apps for which such ad controls would not be applicable.

11.3.5 Drivers and barriers to adoption

As with most consumer web tools, the drivers for adoption tend to be increased awareness and consumer education around data privacy issues.

11.3.6 Future developments

The decision by the Chromium Project to phase out of third-party cookies by 2022, together with existing default blocking of these cookies on Safari and Firefox, will significantly limit the ability of the open display advertising market to continue current practices of targeting advertising based on personal data. Participants in the open display advertising market are currently developing alternative targeting approaches. The Google Chromium Privacy Sandbox[305] floats the idea of a 'federated learning of cohorts' approach to interest-based targeting, among other concepts. This idea would enable targeting at the level of anonymised groups of people.

[305] https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

In the open display advertising market, consumers are likely to be exposed to less advertising targeted based on personal data, and potentially more advertising targeted based on context. This development will reduce the likelihood of consumer harm from discriminatory targeting or targeting vulnerable people. However, phasing out third-party cookies will not affect targeting practices in certain logged-in environments, such as social media platforms.

Contextual targeting is likely to become increasingly prevalent, with advertisers selecting placements on the basis of content relevance. Publishers with logged-in users may develop audience segments derived from first-party data, allowing advertisers to continue to target interest-based segments, but within isolated "walled gardens" only. The industry is also developing solutions to match publisher and advertiser data in a privacy compliant way – to enable targeting on advertiser and publisher first-party data. Technology vendor Infosum provides a Unified Data Platform that enables market participants to query each other's first-party data in a privacy compliant way.[306]

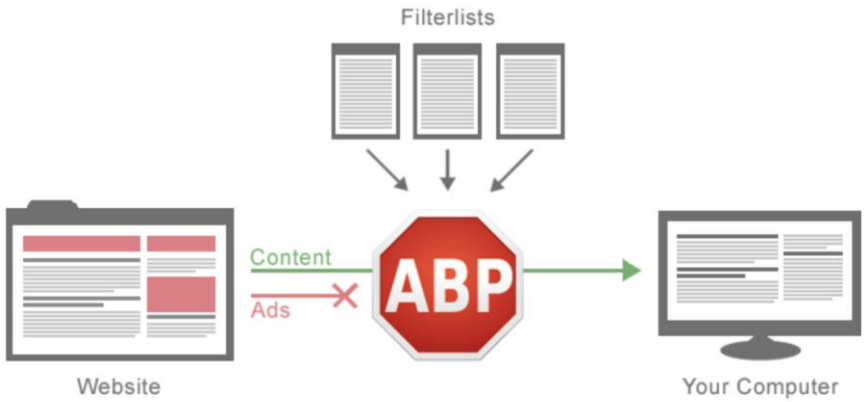
11.4 Ad blockers

Ad blockers are software which allow users to alter or remove online advertising content from a web browser, website or mobile app. To the extent that users are able to reduce their exposure to online ads, ad blockers limit exposure to various forms of inappropriate advertising and inappropriate targeting. However, ad blocking does not address the underlying causes of these online advertising issues.

11.4.1 Objectives

An ad blocker is a software used either to remove or to alter online advertising content from a web browser, website or mobile app (Figure 11.9). It is usually applied as a browser extension or as an app, and blocks either all ads or only the ads that it considers as non-acceptable. Users can also customize the type of ad content they want to blacklist or whitelist. The main benefits to individual users include faster page load times, improved device performance, privacy protection and more secure web browsing, by blocking malicious ads that seek to infect devices.

Figure 11.9: Adblock Plus filters out elements of a website from being loaded or displayed



Source: Medium[307]

[306] https://www.infosum.com/platform/platform-overview
[307] Medium/Connor Finnegan (January 2019). *How ad blockers work and what they mean for web developers*. Available at https://medium.com/better-programming/how-ad-blockers-work-and-what-they-mean-for-web-developers-f151fd73ec28

11.4.2 Description

Ad blocking tools can be browser extensions or stand-alone applications. Some popular free ad blockers are:

- Adblock Plus (ABP) (extensions available on Chrome, Edge, Firefox, IE, Opera, Safari, Android, iOS)
- AdBlock (extensions available on Chrome, Firefox, Safari, Edge)
- AdBlocker Ultimate (extensions available on Chrome, Firefox, Opera)

Based on statistics on the Chrome Web Store,[308] both Adblock Plus and AdBlock extensions have more than 10 million users globally while Firefox reports around 9.4 million users for Adblock Plus.[309] Most popular ad blockers can also be used on both desktop web and mobile web browsers.[310]

Ad blockers operate in various ways:

- Some ad blockers block all ads and some block part of them. Users can keep the default block list, subscribe to additional ones, create their own and whitelist their favourite websites. Blocking rules can be by address parts, by domain name, or for the exact address.[311]
- Some restrictions are based on the nature of the element itself and how it behaves on the page and others state that the ads can only take up a certain percentage of the page.
- Some ad blockers will replace the blocked ad by another content, some others will leave the space blank or a broken link.

The mechanisms used are:

- HTTP request blocking (if the ad is stored on another server): If the site attempts to load the ad from a banned domain or with the wrong keywords, the ad blocker will block the http request.
- CSS filter (if the ad is stored on the site itself): The ad blocker applies a CSS filter to prevent the ad from displaying on the page.

In both cases, the underlying mechanism is that when the web page is loading, the ad blocker screens the script and compares it to the list of banned domains and keywords it must block. These programs work by caching and filtering content before it is displayed in a user's browser. For instance, Adblock Plus considers the following as non-acceptable ads:

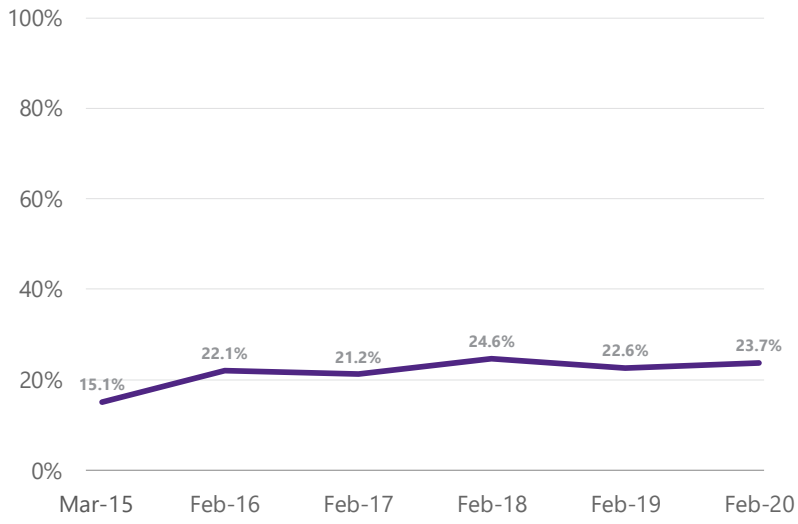
[308] https://chrome.google.com/webstore/category/extensions?hl=en-GB
[309] https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/
[310] For instance, there are several versions of Adblock Plus for mobile browsers including 'Adblock Plus for Samsung Internet', 'Adblock Plus for Safari (iOS)', and 'Adblock Plus for Firefox (Android)'.
[311] For more information, see https://adblockplus.org/filter-cheatsheet

- Ads that visibility load new ads if the primary content does not change
- Ads with excessive or non-user-initiated hover effects
- Animated ads
- Autoplay-sound or video ads
- Expanding ads
- Generally oversized image ads
- Interstitial page ads
- Overlay ads
- Overlay in-video ads
- Pop-ups
- Pop-unders
- Pre-roll video ads
- Rich media ads (e.g. Flash ads, Shockwave ads, etc.)

11.4.3 Adoption

The IAB UK which tracks ad blocking levels estimates that as of 2020 usage of ad blocking is 23.7% among UK online adults (this is based on online adults who have ever downloaded an ad blocker and are currently using one).[312] The level of ad blocking usage has remained relatively stable since 2016 as illustrated in Figure 11.10.

Figure 11.10: Usage of ad blocking software among UK online adults

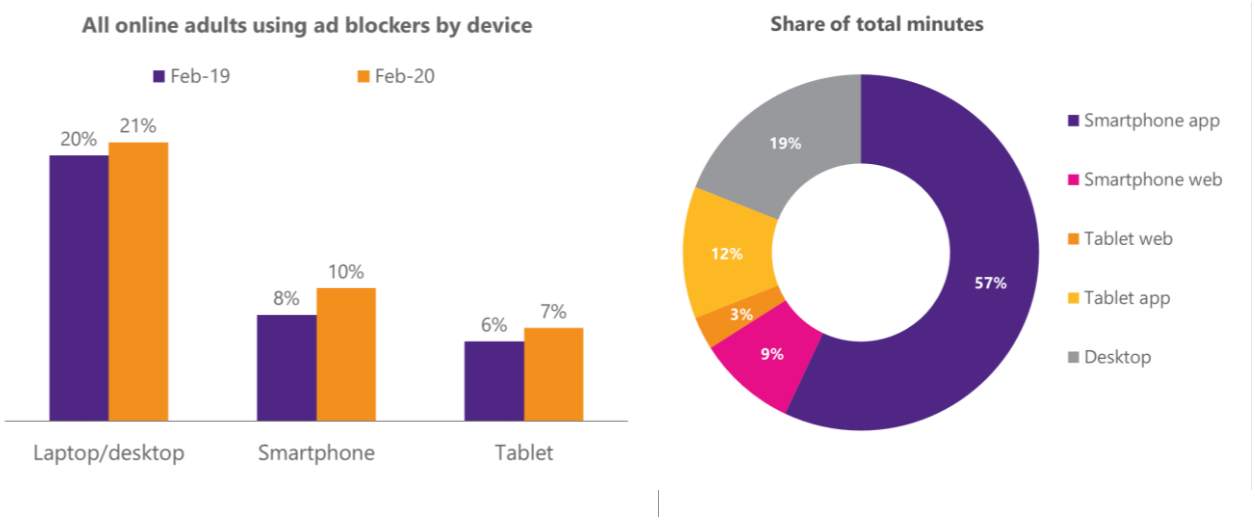


Source: IAB, YouGov

The usage of ad blockers varies by device. Despite the shift of ad revenues towards mobile in recent years, there has not been a significant shift towards the use of mobile ad blockers. As shown in Figure 11.11, desktop/laptop account for significantly less time spent online by users compared to smartphone. In particular, app usage on smartphone and tablet make up two-thirds of time spent online, and this tends to be the environment where ad blocking use is lowest.

[312] IAB UK (2020). *Ad Blocking: tracking ad blocking levels in the UK.* Available at https://www.iabuk.com/research/ad-blocking-2020

Figure 11.11: Usage of ad blockers usage versus time spent by device



Source: IAB, YouGov, Comscore

11.4.4 Efficacy

Based on the IAB's 2019 survey,[313] most users of ad blockers do so 'to block all types of ad' (40%) with other reasons including

- To block certain types of ads (7%)
- To block adverts on certain websites (10%)
- To avoid getting a virus (10%)
- To protect my privacy (9%)
- To improve the performance of my device (9%)

Separately, Ofcom has also noted that consumers in the UK are more concerned about online ads slowing down their computer or mobile than showing inappropriate content or directing them to illicit websites or downloads.[314] Consumers surveyed have also indicated that they would be less likely to use ad blockers in exchange for a better online ad experience.[315]

Given the motivations for their usage and the relatively low adoption on mobile devices in the UK, the efficacy of ad blockers in addressing the consumer issues identified in Section 3.1 is limited. To the extent that all or most ads are blocked, individual users are protected from the various forms of inappropriate advertising and inappropriate targeting. However, ad blocking does not deal with the causes of these online advertising issues.

[313] IAB UK (February 2019). *Ad Blocking: consumer usage and attitudes*. Available at https://www.iabuk.com/research/ad-blocking-2019
[314] Ofcom (December 2017). International Communications Market Report 2017.
[315] IAB UK (February 2019).

11.4.5 Future developments

It is unclear whether ad blockers will continue to be relevant given the developments in relation to the default blocking of third-party cookies on browsers as discussed in Section 11.3 and ongoing improvements in online ad experience through industry standards and initiatives (Section 7). Ad blocking may still be useful to privacy-conscious users but indications are that better advertising experience and increased awareness of the value exchange may reduce the need for ad blockers in future.

12 ASA initiatives

As part of its More Impact Online strategy, the ASA is increasing proactive monitoring of online advertising and engaging with industry stakeholders to develop good practices. This strategy describes the enforcement element of this proactive approach as follows:

> **"Through better cooperation, more technological tools (including machine learning) and more resources, we will improve our identification and removal of irresponsible ads (particularly online) and our sanctioning of non-compliant advertisers"**[316]

ASA initiatives in this area employ ground-breaking techniques and are ahead of many of its peers internationally. To large extent, these initiatives are experimental, and the ASA is in a test and learn phase. The following sections present a snapshot of recent and planned activity and an indication of the direction of travel for this work.

12.1 ASA avatars 2018

12.1.1 Objectives

The ASA's avatar research aims to monitor categories of online advertising that consumers, especially under 18-year olds, are exposed to in order to identify breaches of the Advertising Codes. To date, the avatars have been used to identify gambling ads on sites aimed at children and to monitor HFSS ads on general websites and YouTube channels.

12.1.2 Description

In November 2018, the ASA commissioned Advertising Intelligence Ltd, a subsidiary of global marketing and media analytics company Nielsen, to monitor categories of online display ads served to UK consumers. This monitoring exercise used 'Avatars', constructing online profiles which mimic the online browsing profiles of an internet user of a particular age profile.

The avatars are computer programmes that browse online content in an automated way. Each avatar was designed to exhibit the characteristics of a specific type of internet user, including a child, a teenager, an adult, a child and an adult sharing a device. Each of these avatars created a relevant data trail by visiting a selection of 20-25 age-specific sites in order to receive cookies. A retargeting avatar was programmed to visit a selection of HFSS, gambling and alcohol brands in order to develop a data trail that could be used by these brands to retarget users with ads while browsing unrelated websites.

The avatars were programmed to visit 210 popular websites and 40 YouTube channels twice daily over a two-week period. These websites were selected for appeal to a general audience (105 sites) or for 'youth interest' (105 sites). YouTube channels were primarily 'youth interest'. The avatars did not visit logged in environments, such as social media platforms, or apps or audio streaming services.

The avatars captured details of over 95,000 banner, display and video ads served to them. Each ad was then categorised to establish the brand and the nature of the product being advertised. Ads in the categories of

[316] Advertising Standards Authority, *More impact online, Corporate Strategy 2019-2023*

food, soft drinks, food retail, gambling and alcohol were individually logged.[317] This data then allowed the identification of breaches of the advertising codes.

12.1.3 Effectiveness

The avatars provide evidence of instances in which children, engaging in online environments of particular appeal to children, have the potential to be exposed to age-restricted advertising in clear breach of the Advertising Codes. Avatars do not provide data about the incidence of such mis-targeted advertising, given that avatar behaviour differs from real-life consumer browsing in various respects:

- Volume of page and video views – the avatars viewed content at a higher rate than real consumers. In consequence, the avatars are likely to be exposed to a wider variety of ads than real-life consumers who generate fewer impressions and may be served a small selection of campaigns.

- Data trail – the avatars created a limited data trail over a short period, including only website browsing data. But real consumers create a rich online and offline data trail consisting of searches, click-throughs, purchases, declared interests, advertiser customer databases and many other factors.

The avatars research showed that 23 gambling ads were seen by the child avatars 151 times on children's websites – 1.4% of the 10,754 ads they saw on those sites. As a result of this research, the ASA took action to ban ads from five gambling operators which were served to child avatars on children's websites – including colouring-in and dress-up game sites. To follow up on these findings, the ASA engaged with advertisers to detail the nature of the non-compliance and to promote the uptake of best practice tools to support targeting away from media targeting or appealing particularly to under 18-year olds.

The research also found that 947 (2.3%) of ads served to child avatars on child sites and YouTube channels were for HFSS products, though two-thirds of these ads were for products likely to be of little interest to children. 43 ads for HFSS products were served on 13 websites clearly aimed at children, though no HFSS ads were served on 26 other websites aimed at children. Ads for HFSS products also appeared on 20 out of 21 YouTube channels that were clearly aimed at children.

12.2 Emerging monitoring work

The ASA is continuing to develop its proactive monitoring through a range of research initiatives, including:

- **Quarterly monitoring of advertising on websites aimed at children**. The ASA will use automated methods to monitor the advertising served on a selection of sites that appeal to children, excluding logged-in environments such as social media services. This research will identify advertising in categories such as gambling and e-cigarettes that is mis-targeted to children. It is anticipated that the regularity of this monitoring will encourage brands to comply with the advertising codes in relation to targeting of children.

- **Avatar monitoring of children in mixed-age audience environments**. This avatars research will monitor ads served to audience segments that are likely to comprise under 18-year olds in online environments that appeal to mixed age audiences, and identify instances of ads for age-restricted products such as HFSS.

[317] Data collected included data and time served, URL of the page/video visited (and a screenshot of the ad in context), the URL of the landing page resulting from clicking on the ad, whether the ad was seen on mobile or desktop, the positioning of the ad (e.g. banner; mid-page; wrap-around; pre-roll video).

- **Monitoring of advertising within logged-in environments.** The ASA is exploring potential approaches to monitor advertising on services that require a login, such as Facebook, Instagram and Snapchat. In these environments, the monitoring might cover ad content and targeting.

- **Research into adult vulnerability**. The ASA is at the early stages of research into how vulnerable adults may be targeted by advertising, based on engagement with experts and a review of secondary research sources.

In addition, the ASA is investing in technology to provide ongoing monitoring of some forms of online advertising. It is using a third-party tool to identify certain ad content on social media that is in clear breach of the advertising codes, such as beauty salon ads for Botox treatments. The ASA is also investigating the potential for data science and machine learning to identify instances of advertising in breach of the advertising codes, such as non-labelling of social influencer marketing

12.3 Engagement with platforms

The ASA is also engaging with social media platforms and participants in the open display supply chain to encourage good practices. Areas of activity include scam ads, where participants are working with the ASA to ensure swift take down of scam ads and information sharing between players. Industry stakeholders are also engaging with the ASA around standards for online advertising, such as aligning platform policies with the advertising codes.

13 Effectiveness of the current system

The advantages of self-regulation rest mainly on considerations of expertise and efficiency. Within the advertising industry in general, self-regulatory systems are well established and widely practised around the world, and to a large extent they have worked well so far. The ASA, with its longstanding experience and extensive expertise across different forms of advertising, sales promotions and direct marketing communications, is well placed to ensure regulatory effectiveness in terms of voluntary compliance. It has also been quick to adapt rules in light of the changing nature of the advertising, particularly in the online environment, and evolving social norms and issues such as mental health. Ongoing ASA activities as discussed in Section 12 demonstrate its ability to stay abreast of emerging issues and key areas of concern.[318]

The effectiveness of self-regulation depends crucially on the incentives to participate. In the online environment the emergence of new forms of data-driven advertising and social media has introduced a host of new players across a complex ecosystem, and as mentioned Section 6.1 above, the incentives for these players may not be aligned along common interests. For instance, bad actors intent on causing harm through malicious advertising have little or no incentive to abide by industry standards and CAP Code regulations. In the growing social influencer segment, individual influencers may be less aware of potential issues and may not see the need to abide by the relevant guidelines.

The risk is that consumers may not receive adequate protection in a self-regulatory system which controls the most responsible members of an industry but potentially leaves unregulated individuals or firms least inclined to serve public or consumer interest due to gaps in the system. In this regard, we identify the following areas for improvement.

- Lack of a coherent consumer protection framework for online advertising issues. There are two related aspects to this.
  - First, there is room for a more coordinated and clearly signposted mechanism for consumers to report inappropriate advertising and to help consumers understand the available options and process for redress. At present, there is a confusing patchwork of reporting methods and this makes it difficult for consumers seeking redress.[319]
  - Second, there are overlaps in regulatory structure and responsibilities which makes enforcement potentially difficult and time consuming. Various agencies with different and overlapping remits have an interest in the online advertising sector;[320] and no one single organisation has all the necessary expertise, information and/or powers to effectively address some of the areas of harm identified. This is a fast evolving industry where issues can emerge and change. Also, the nature and causes of some of these harms go beyond just online advertising[321] which underlines the need for closer coordination between regulatory agencies to improve regulatory efficiency and effectiveness.
- Better data for monitoring purposes. Other than ASA complaints data, there is no easy way to monitor and measure the performance of the self-regulatory system. More data sharing, ideally in a standardised format, by players in the online advertising value chain with the relevant agencies will help promote accountability and transparency.[322] We note also that the ASA as a self-regulator does not have

[318] The ability to fund activities in these new areas may be limited by the funds available which are raised through a voluntary levy on advertisers.
[319] The nature of harms varies and affect consumers in different ways and complaints can be made through various channels such as the ASA, Trading Standards, Citizens Advice and Action Fraud, as well as through online platforms, such as Facebook, Google and Instagram.
[320] These include the ASA, Action Fraud/National Fraud Intelligence Bureau, Citizens Advice, CMA, ICO and Trading Standards.
[321] Related to this is a definitional issue – online advertising overlap with online content, for example in the area of organic social media posts which are not covered by the ASA. It is clear that some areas of consumer harms in online advertising are also associated with online content more generally. Activities to protect consumers and the wider public in the online environment may need to take both aspects into account.
[322] The retention of ads will allow analysis of past activities and trends, and may be a possible option to consider.

information-gathering powers which are underpinned by legislation and this is an area which may require cooperation with other agencies with an interest in the sector.

- Lack of regulatory oversight of online platforms. The CAP Code applies to advertisers but not online platforms. We note that these platforms have detailed policies and guidelines on advertising and general online content which are generally aligned with the CAP Code and industry agreed practices. However, there could be more clarity on how these policies and guidelines are enforced and whether they have had significant impacts on the issues they are meant to address.

- Limitations of the incentive-based system. Major advertisers and platforms are held to account by concerns around their reputation and, in the case of advertisers, their ability to continue advertising. These incentives hold less sway over overseas advertisers, short-term advertisers and bad actors.

- Underdeveloped guidance around potential issues associated with targeting, such as discrimination and inappropriate targeting. Presently, the main codification of rules is around the mis-targeting of advertising to children. This could be an area for further investigation.

- Limited scope and reach of consumer awareness and public education initiatives. Expanding these programmes can help raise awareness of online advertising issues and the available tools and options to address some of them. We note that the ASA and advertising industry have identified raising public awareness as part of their strategies.[323,324]

[323] ASA (1 November 2018). More Impact Online: the ASA's 2019-2023 Strategy. Available at https://www.asa.org.uk/uploads/assets/uploaded/96455868-e7b1-4ac7-8185f37893fd6f0d.pdf
[324] Advertising Association (March 2019). Arresting the Decline of Public Trust in UK Advertising. Available at https://www.iabuk.com/sites/default/files/public_files/AA_Public_Trust_Paper.pdf

Appendix A Glossary

Ad impression. A metric expressing each time an ad is served and displayed, whether it is seen or not, whether it is clicked on or not.

Ad inventory. The amount and types of ad space a publisher has available for an advertiser to buy.

Ad optimisation. A means of improving campaign performance through automated and semi-automated means, usually through a systematic approach. Ad optimisation often focuses on cost (especially prices in automated bidding), targeting or creative, gleaning performance improvements through testing.

Advertising technology (Ad Tech). An umbrella term that describes systems of analysing and managing tools for programmatic advertising campaigns.

AdChoices Icon. An interactive symbol that links consumers to an online portal which provides information on data-driven advertising and a mechanism for exercising informed choice over tailored, personalised ads. This is an initiative by the European Interactive Digital Advertising Alliance (EDAA) which manages the European self-regulatory programme for online behavioural advertising.

Avatar. A programme that simulates an online profile of a user, in order to identify ads served to this profile across the internet.

Botnet. A botnet refers to a group of computers which have been infected by malware and have come under the control of a malicious actor. Botnets can be designed to accomplish illegal or malicious tasks including sending spam, stealing data, ransomware, fraudulently clicking on ads or distributed denial-of-service (DDoS) attacks.

Brand safety. The set of measures that aim to protect a brand's image from the negative or harmful influence of inappropriate or questionable content on the publisher site where an ad is served.

Browser extension. A small software module for customising a web browser.

Cascading Style Sheets (CSS). A style sheet language used for describing the presentation of a document written in a mark-up language like HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript.

Cookie. A cookie, also known as an HTTP cookie, web cookie, or browser cookie, is a string of text sent from a web server to a user's browser that the browser is expected to send back to the web server in subsequent interactions.

Demand-side platform (DSP). A service provider that enables media agencies, trading desks or advertisers to buy programmatic display advertising from sources of supply including ad exchanges, supply-side platforms and media owners.

Distributed Ledger Technology (DLT). A way of digitally recording transactions across a distributed (peer-to-peer) network of computers so that any record involved cannot be altered retroactively.

Domain spoofing. A practice where dishonest publishers, ad networks or exchanges obscure the nature of their traffic to resemble legitimate websites.

Facebook Audience Network. Facebook's advertising network which allows advertisers to extend their Facebook and Instagram campaigns to other mobile apps or platforms.

HTTP request. HTTP (Hypertext Transfer Protocol), is the underlying format that is used to structure requests and responses for effective communication between a client and a server. The message sent by a client to a server is known as an HTTP request.

Javascript. A scripting or programming language that allows the implementation of complex features on web pages.

Force redirect. A mechanism through which a user is redirected to unwanted destinations which might include malware downloads, scam websites or fake ads designed to collect personal information.

General Data Protection Regulation (GDPR). A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

Interstitial. A web page displayed before or after an expected content page, usually to display advertisements. Most interstitial advertisements are delivered by an ad server.

Malvertising. The use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages.

Malware. Software which is intentionally designed to cause damage to a computer, server, client, or computer network.

Online behavioural advertising. A form of targeted advertising in which advertising networks work with websites and advertisers to deliver customised advertising based on the collection and use of consumers' web browsing activity.

Pop-up ads. Ads which pop up and block the main content of the page.

Postitial ads. Ads which appear after a user follows a link.

Prestitial ads. Ads which appear before the content of the page has loaded, temporarily blocking the user from continuing on to the content they have sought out.

Programmatic. Programmatic trading is the use of automated systems and processes to buy and sell inventory. This includes, but is not limited to, trading that uses real time bidding auctions.

Publisher. We use the term publisher broadly to refer to any online operator that attracts an audience to content it provides.

Retargeting. A form of online advertising which targets consumers based on their previous actions using cookie-based technology.

Social media. Social media are interactive computer-mediated technologies that facilitate the creation and sharing of information, ideas, interests and other forms of expression via virtual communities and networks.

Social plug-ins. Tools that let users share experiences on other websites with others on social media platforms. Examples include the Like button, the Share button and comments.

Supply-side platform (SSP). A technology platform used by publishers to automate the sale of online advertising inventory. SSPs connect publishers to multiple sources of demand, including DSPs and other SSPs.

Tracking pixel or pixel. A 1x1 pixel-sized transparent image that provides information about an ad's placement. In many cases, a tracking pixel is used to notify an ad tracking system that either an ad has been served (or not served, in some cases) or that a specific web page has been accessed. Also known as a beacon, web beacon, action tag or redirect.

User ID. A user ID is a unique customer identifier by which a publisher identifies a user visiting its website – usually including only pseudonymous data.

Viewability. An online advertising metric that aims to determine only impressions that had the opportunity to be seen by users. For example, if an ad is loaded at the bottom of a web page but a user does not scroll down far enough to see it, that impression would not be deemed viewable. Viewability is not a measure of ad effectiveness.

Appendix B Stakeholder engagement

The stakeholder engagement exercise for this study was conducted from February to March 2020, involved a series of interviews and follow-up email correspondences with relevant industry bodies, technology vendors, publishers and platforms, and public sector agencies. In total, 15 stakeholders contributed to our research and we are grateful for their valuable inputs.

Figure B.1: Stakeholders inputs for the study

Category	Stakeholder
Industry bodies	• Advertising Standards Authority (ASA) • The Internet Advertising Bureau (IAB) UK • Advertising Association • Joint Industry Committee of Web Standards (JICWEBS) • European Interactive Digital Advertising Alliance (EDAA) • Trustworthy Accountability Group (TAG)
Technology vendors	• The Media Trust • Fiducia • A cybersecurity company specialising in the digital ad ecosystem
Publishers and platforms	• Google • Facebook • A major UK news publisher
Public sector agencies	• Action Fraud/National Fraud Intelligence Bureau (NFIB) • Information Commissioner's Office (ICO) • National Trading Standards

Appendix C Examples of ad fraud

Figure C.1 provides examples of specific cases and types of fraud. These cases were identified in the USA, but their reach is international.

Figure C.1: Examples of ad fraud

Example	Fraudulent practices involved			
	Fake traffic	Fake audience data	Fake context	Fake actions
3ve botnet fraud. In 2018, the US Department of Justice announced that it had dismantled two international cybercriminal rings and indicted 8 defendants for causing tens of millions of dollars in losses in digital advertising fraud.[325] The fraud involved three main components. First, fraudsters used malicious advertising to infect at least 1.7 million Windows computers with malware creating a botnet. Second, they set up bots in data centres to produce fake traffic that was passed through the infected computers in the botnet. Third, the fraudsters sold some of this fake traffic to third parties who wanted to commit ad fraud. They also used the fake traffic to view ads on about 5,000 counterfeit websites that used domain spoofing to masquerade as high-quality legitimate websites.[326]	●		●	
"DiCaprio" fraud. In January 2020, Pixalate identified an ad fraud scheme in which fraudsters bought display ad impressions on the dating app Grindr, then delivered Javascript into these ads to initiate spoofed ad requests for video ads claiming to originate from a Roku app on a Roku device.[327] Advertisers purchased this fake video ad inventory can cost as much as 25 times more than the mobile banners purchased by the fraudsters.[328]			●	
Location fraud – general case. Security vendor Location Sciences found that some app developers create fake GPS signals in order to accrue greater advertising revenues.[329] This form of fraud deceives advertisers into thinking that mobile ad impressions are served in particular locations they value, such as in proximity to retail or fast food outlets. Location Sciences estimate that up to 90% of these signals in the programmatic ad tech stack are fake. However, they do not provide information about specific cases.		●		

[325] https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing
[326] https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown
[327] https://blog.pixalate.com/dicaprio-ott-ctv-ad-fraud-scheme-grindr-mobile-app
[328] https://www.buzzfeednews.com/article/craigsilverman/grindr-roku-apps-ad-fraud-scheme
[329] Location Sciences, The State of Location Advertising, 2019.

Example	Fraudulent practices involved			
	Fake traffic	Fake audience data	Fake context	Fake actions
Uber - victim of click attribution fraud. In 2019, Uber announced that it was suing five ad networks for purchasing non-existent, non-viewable or fraudulent advertising.[330] One aspect of this claim is that Uber's suppliers reported fake clicks that never actually occurred, clicks on fake or malicious websites, clicks from stacked ads which were not all viewed by users, auto redirect "clicks", and clicks on deceptive ads, such as those designed to look like smartphone keyboard buttons. Uber operates a performance marketing model in which it pays for clicks that result in installation of the Uber app, new sign ups and/or first trips. Uber used a third-party attribution provider to analyse results and clicks in order to credit the network or publisher responsible for the last click. The fraudulent clicks enabled networks to falsely claim credit for results, and thereby payment. Since 2015, Uber paid out about $70 million for mobile advertising placed by the defendants in the case.				●

[330] https://www.adexchanger.com/wp-content/uploads/2019/06/Uberfraudsuit.pdf