

Advertising and the Online Safety Act 2023

Lorna Woods & Alexandros Antoniou

To cite this article: Lorna Woods & Alexandros Antoniou (05 Feb 2026): Advertising and the Online Safety Act 2023, Journal of Media Law, DOI: [10.1080/17577632.2025.2606428](https://doi.org/10.1080/17577632.2025.2606428)

To link to this article: <https://doi.org/10.1080/17577632.2025.2606428>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 05 Feb 2026.



Submit your article to this journal [↗](#)



Article views: 668



View related articles [↗](#)



View Crossmark data [↗](#)

Advertising and the Online Safety Act 2023

Lorna Woods and Alexandros Antoniou 

Essex Law School, University of Essex, Colchester, UK

ABSTRACT

Online advertising's increasing opacity and automation have exposed critical limitations in the current regulatory structures, particularly regarding fraudulent content and ad misplacement. This contribution argues that the Online Safety Act 2023 (OSA) marks a partial shift by extending duties to user-to-user (U2U) and search services for addressing fraudulent ads (OSA Part 3, Chapter 5), but the scope of these responsibilities remains unclear. Key definitional ambiguities, particularly around 'user-generated content', 'users' and 'services', threaten to confuse the regime's enforcement potential in this context and undermine the coherence of these new obligations. Whether advertisers fall within the scope of 'users' under the Act critically shapes the application of general safety duties to advertising, raising unresolved questions about the reach of illegal content provisions across different types of services. The Act's exemption of search services from broader duties on illegal content in paid-for ads further entrenches enforcement asymmetries between regulated services despite equivalent exposure to harm. While the Online Advertising Programme (OAP) was conceived to address systemic regulatory blind spots, its limited focus on content, rather than delivery infrastructure, has stalled meaningful reform. The article concludes that the OSA introduces vital duties but falls short of delivering a comprehensive regulatory framework, leaving some gaps in coverage, enforcement, and oversight of third-party ad delivery systems.

ARTICLE HISTORY Received 31 July 2025; Accepted 12 December 2025

KEYWORDS Online Safety Act 2023; fraudulent advertising; programmatic advertising (ad tech); platform duties; Ofcom Codes of Practice

Introduction

Advertising is a significant element of the online environment, yet concerns persist about the extent to which it is adequately regulated. Part of the problem arises from the fact that advertising in the online space gives rise to issues across two aspects. The first concerns its content, particularly

CONTACT Alexandros Antoniou  a.antoniou@essex.ac.uk

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

around scams and fraud. A sub-set of content concerns is the blurred line between organic content – user posts or material appearing without paid placement (i.e. not boosted through an ad system; term used descriptively, not as a statutory category) and commercial/ sponsored material, including influencer promotions. There are growing apprehensions that platforms’ responses to complaints about such ads are often slow or ineffective.¹ The second concerns ad placement, where ads appear alongside terrorist content, child abuse material or misinformation and made-for-advertising (MFA) websites (i.e. sites designed primarily to exploit ad monetisation algorithms, offering low-value, click-driven material).² Such problematic placements underline concerns recently highlighted by the Commons Select Committee Report on Social Media, which noted ‘[t]he algorithmic spread of false and harmful content is closely linked to the digital advertising market’.³ Related concerns include scam sites that exploit obituary content (not always MFA by design, but sometimes monetised through similar ad-heavy structures), where personal information from death notices is misused for fraud.⁴ In this piece, these placement and visibility issues, often involving manipulation of ad placement systems and improper ad delivery, can be referred to as ‘ad fraud’ in programmatic systems.⁵ Targeting-bias and data protection issues are excluded and lie outside this article’s scope.⁶ By contrast, we capture any deceptive paid-for advertising that either contravenes the criminal law or misleads consumers in ways that breach trader-conduct rules or sector-specific regimes (e.g. unlawful financial promotions) as ‘fraudulent ads’, which we use here as a wider, analytic label to map the problem space. As will be seen, where the Online Safety Act 2023 (OSA) applies, it uses a narrower statutory, closed list of related criminal offences (so, our labelling is intended to organise the analysis and does not expand the Act’s compliance triggers).

¹Which?, ‘Scam Adverts: Are You Still being Targeted?’ (27 February 2024) <www.which.co.uk/news/article/scam-adverts-are-you-still-being-targeted-a4jj68Q8cQcm> accessed 30 June 2025.

²Internet Advertising Bureau UK, *A guide to identifying Made for Advertising websites* (17 July 2023) <www.iabuk.com/sites/default/files/public_files/MFA_guide.pdf> accessed 27 June 2025; see also Adalytics, ‘Are Amazon and other ad tech vendors serving ANA members’ ads on “Made for Arbitrage” websites in 2024?’ <<https://adalytics.io/blog/ads-observed-on-made-for-advertising-sites-in-january-2024>> accessed 26 June 2025.

³Science, Innovation and Technology (SIT) Committee, *Social Media, Misinformation and Harmful Algorithms* (HC 2024–25, 441) para 79.

⁴Secureworks Counter Threat Unit, ‘Are Scammers using AI to Enhance Fake Obituary Sites?’ (21 March 2024) <www.secureworks.com/blog/are-scammers-using-ai-to-enhance-fake-obituary-sites> accessed 30 June 2025.

⁵See also Interactive Advertising Bureau Europe (IAB Europe), *The IAB Europe Guide to Ad Fraud* (December 2020) <<https://iab europe.eu/wp-content/uploads/IAB-Europe-Guide-to-Ad-Fraud-1-2.pdf>> 25 June 2025.

⁶Information Commissioner’s Office (ICO), ‘Investigations Announced into How Social Media and Video Sharing Platforms Use UK Children’s Personal Information’ (3 March 2025) <<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/02/investigations-announced-into-how-social-media-and-video-sharing-platforms-use-uk-children-s-personal-information/>> accessed 27 June 2025.

These concerns about deceptive ad content (scams and misleading claims) and ad placement/ delivery risks track two architectures of delivery. Broadly, display advertising operates either through 'walled garden' environments (such as those run by Meta, Google or Amazon), where platforms sell and serve their own ad inventory using proprietary tools in closed, integrated systems; or through the open display market, where publishers rely on complex chains of ad tech intermediaries and programmatic trading (this leverages real-time audience data to automate the buying and selling of digital ad space).⁷ These distinct architectures carry different risks and afford different levels of control: while 'walled gardens' operate integrated ad tech systems and oversee much of the ad transaction internally, publishers in the open display market are often at the receiving end of opaque and fragmented supply chains,⁸ with limited ability to vet ads or manage ad placement. The Select Committee on Social Media underlined this opacity too, citing the 2024 UN Global Principles for Information Integrity, which describe digital advertising processes as complex and minimally supervised, with the result that advertising budgets can inadvertently funnel funding to actors or ideas that advertisers would never knowingly endorse.⁹

Recent research underscores the scale and persistence of the risks to which advertising might give rise.¹⁰ From an advertiser-facing angle, these risks matter because they expose delivery-side integrity issues that in turn can elevate the risk of users' exposure to illegal content that may engage OSA obligations. There are also questions about whether ads even reach their intended audience,¹¹ given techniques that distort performance data and cause wasted ad spend, namely advertiser expenditure on paid impressions or clicks without a genuine human opportunity to see, like bot traffic (where automated software mimics human users to inflate ad metrics), pixel stuffing (hiding ads in invisible pixels so users never actually see them) and ad stacking (layering multiple ads on top of each other in a single ad slot, with only the top one visible but all counted as 'served').¹²

⁷For further detail, see Lorraine Conway, *Online Advertising* (Research Briefing Number 9510, House of Commons Library, 12 December 2022) <<https://researchbriefings.files.parliament.uk/documents/CBP-9510/CBP-9510.pdf>> accessed 8 July 2025.

⁸Damien Geradin and Dimitrios Katsifis, 'An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age' (2019) 15(1) *European Competition Journal* 55.

⁹SIT Committee, *Social Media, Misinformation and Harmful Algorithms* (n 3) para 86.

¹⁰Adalytics, 'Full Report: Are Ad Tech Vendors Facilitating or Monitoring Ads on a Website that Hosts Child Sexual Abuse Material?' <<https://adalytics.io/blog/adtech-vendors-csam-full-report>> accessed 30 June 2025.

¹¹Pixelate, 'Pixelate Releases Q3 2024 Global Click Fraud Benchmarks Reports for Mobile Apps, Desktop Web, & Mobile Web' (29 October 2024) <www.pixelate.com/blog/q3-2024-click-fraud-benchmarks-reports> accessed 30 June 2025.

¹²See further Competition and Markets Authority, *Online Platforms and Digital Advertising Market Study* (3 July 2019, updated on 1 July 2020) <www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report> accessed 24 June 2025. Also refer to industry standards used to distinguish human, viewable opportunities to see from invalid or non-viewable delivery in IAB Europe's *Retail Media Measurement Standards* on 'sophisticated invalid traffic' (August 2024) 6 <<https://iab europe>.

Compounding these issues are structural weaknesses: a lack of transparency in ad trading and audience measurement, inadequate vetting that allows malign actors into the supply chain, and the constant evolution of sophisticated fraud tactics which evade detection.¹³ The largely automated and opaque ad delivery system, particularly in the open display market, is susceptible to exploitation by fraudsters, unscrupulous publishers, or even opportunistic intermediaries, seeking to exploit the system's vulnerabilities – an area where content regulation exists but oversight of delivery infrastructure remains limited. Advertisers who purchase fake ad placements are the direct victims of such fraud, while genuine publishers face revenue losses as advertising funds are diverted toward counterfeit inventory.¹⁴ There are concerns that persistent erosion of trust could eventually stall innovation and weaken advertisers' confidence in digital ecosystems.¹⁵ In this, concerns may differ between 'walled garden' advertising environments (e.g. Meta's delivery of ads on its own services) and the open display market. These two systems may also be treated differently in regulatory terms.

Against this backdrop, this article reviews the existing regime and delineates how the OSA's fragmented definitions and selective reach weaken its capacity to establish a comprehensive framework for online advertising, with implications for regulatory strategy and platform compliance. We proceed on the premise that the OSA was not conceived as an advertising statute. The question we answer is whether, given the enacted text, it nonetheless yields a coherent, bounded settlement for ads or an unstable, partial one. We argue the latter is the case.

The article first outlines the current baseline advertising framework, which remains content-centric (the only material pre-OSA platform obligations that brushed against placement were those in the Video-Sharing Platform rules, discussed below, but did not impose a general obligation to police programmatic placement across the ad supply chain). It then considers the extent to which the OSA, which addresses social media and search content delivery systems, tackles both ad fraud and fraudulent ads, as well as considering the approach to criminal ads more broadly. The analysis highlights drafting ambiguities in the OSA that cast doubt on whether the policy objective of excluding both ad delivery and ad content from the regime (with the

[eu/wp-content/uploads/IAB-Europe_Retail-Media-Measurement-Standards-2024.pdf](#)> accessed 9 October 2025.

¹³Department for Culture, Media and Sport, *Mapping Online Advertising Issues, and the Industry and Regulatory Initiatives Aimed at Addressing Them* (9 July 2020) 58 <www.gov.uk/government/publications/mapping-online-advertising-issues-and-the-industry-and-regulatory-initiatives-aimed-at-addressing-them> accessed 27 June 2025.

¹⁴*ibid.*

¹⁵Roberto Cavazos, *The Economic Cost of Bad Actors on the Internet* (University of Baltimore/ CHEQ Report, 2019) <www.mmaglobal.com/files/casestudies/cheq_the_economic_cost_of_bad_actors_on_the_internet.pdf> accessed 2 July 2025.

exception of fraudulent ads) is fully achieved. This interpretation opens the possibility of the application of a wider range of priority content rules to ads on social media, while preserving protections against fraudulent ads. The position regarding delivery systems and ad fraud is less clear. Finally, the article questions the role of the Online Advertising Programme (OAP), which was launched by the Johnson administration to review the whole paid-for online advertising ecosystem¹⁶ and subsequently prolonged under Labour,¹⁷ and the extent to which it will fill any gaps left by OSA, specifically around ad fraud. The analysis proceeds as follows: first, we set out the Advertising Standards Authority (ASA)/ Committee of Advertising Practice (CAP) content rules; next, we analyse how the OSA addresses fraudulent ads and where general duties may reach ads; then, we consider the OAP's limited purchase on ad-delivery systems; and finally, we draw the implications.

Regulation of ad content: the existing regime

Advertising content is regulated by the Advertising Standards Authority (ASA), with non-broadcast adverts falling under the CAP code.¹⁸ The non-broadcast category includes the content of adverts provided through social media or other online ad delivery services, and marketing communications in user posts by celebrities and influencers. The CAP Code covers a range of issues – including harm and offence, adverts directed at children, and misleading ads. It also sets out specific rules about certain products or services (e.g. medicines, foods/ food supplements and gambling as well as financial products). A central principle is that marketing communications should be 'obviously identifiable as such'.¹⁹ The ASA describes its aims as ensuring the advertising is 'legal, decent, honest and truthful'.²⁰ The system is principally self-regulatory (although some rules reflect legal obligations and may also fall within the remit of Trading Standards or the Competition and Markets Authority (CMA) as a backstop).²¹ The ASA does not have any powers to fine non-compliant advertisers, nor to compel their

¹⁶Department of Culture, Media and Sport, *Online Advertising Programme Consultation* (25 July 2023) <www.gov.uk/government/consultations/online-advertising-programme-consultation/online-advertising-programme-consultation> accessed 22 June 2025.

¹⁷Department of Culture, Media and Sport, Statement UIN HCWS272 (2 December 2024), *Online Advertising: Taskforce Progress Report 2023–24* <<https://questions-statements.parliament.uk/written-statements/detail/2024-12-02/hcws272>> accessed 22 June 2025.

¹⁸The UK Code of Non-Broadcast Advertising and Direct & Promotional Marketing, <www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html> accessed 30 June 2025.

¹⁹*ibid.*, CAP Code, Section 2, Rule 2.1.

²⁰*ibid.*, Preface.

²¹See *Memorandum of Understanding between the Competition and Markets Authority and ASA on working arrangements in relation to their specific roles in the consumer protection landscape* (21 June 2017) <<https://assets.publishing.service.gov.uk/media/5a824640e5274a2e87dc211d/cma-asa-mou-consumer-protection-issues.pdf>> accessed 7 July 2025.

compliance with their rules, relying instead heavily on industry buy-in and a ‘name and shame’ approach.²² Beyond this, the ASA operates an escalating sanctions regime that includes targeted on-platform ad campaigns calling out repeat offenders; ‘Ad Alerts’ to CAP members (requesting they withhold advertising space from non-compliant marketers), requests to search providers to remove paid-for search ads and pre-vetting requirements for future marketing.²³ For certain consumer protection rules,²⁴ the ASA can make referrals to the Trading Standards authorities, which may take enforcement action under the statutory provisions.²⁵ Note, political advertising, which is subject to specific rules, lies outside the scope of this article.²⁶

One persistent issue pertains to influencers failing to clearly disclose when their content is advertising (i.e. when it has been provided in exchange for payment, gifts, or other forms of value).²⁷ Despite the ASA introducing guidance in 2018 and updating it in 2020, a 2021 monitoring report showed ‘unacceptable levels’ of non-compliance.²⁸ Measures to encourage compliance for traditional formats seemed not to affect influencers. In response,

²²If a marketer publishes non-compliant claims on their own website or unpaid platforms that they control, like social media accounts/ profiles, the ASA may list their name and a description of the issue in a designated section of the ASA website. This listing is search-optimised to appear in online search results until the advertiser rectifies the breach; see further ASA, Sanctions <www.asa.org.uk/codes-and-rulings/sanctions.html> accessed 23 June 2025.

²³For clarity, the ASA cannot compel platforms to impose sanctions but can request action. See further House of Commons Library Research Briefing Number 6130, *Regulation of advertising in the UK* (24 June 2025) section 3.5.

²⁴Digital Markets Competition and Consumers Act 2024 (replacing the Consumer Protection from Unfair Trading Regulations 2008), Part 4, Ch 1, Sch 20, with Trading Standards listed as ‘public designated enforcers’ for civil enforcement under Part 3, Ch 3 (s 151) and equipped with investigatory powers via the Consumer Rights Act 2015, Sch 5 as amended by Sch 21 of the DMCC Act.

²⁵For a list of advertisers recently escalated to the ASA’s legal backstop, Trading Standards, see: <www.asa.org.uk/codes-and-rulings/trading-standards-referrals.html>. Although this does not happen often, the ASA can refer marketers when they fail to comply with its rules and its self-regulatory measures prove ineffective.

²⁶Broadcast political advertising is prohibited by the Communications Act 2003 (s 321); parties instead use party-political broadcasts on TV and radio (s 333), regulated by Ofcom. Non-broadcast political advertising, i.e., material principally aiming to influence voters in elections or referendums, is exempt from ASA regulation under Section 7 of the CAP Code (the ASA will still regulate if the principal function is to sell a product/service). Electoral law sets spending rules and offences (e.g., false statements about a candidate’s personal character), but does not require truthfulness of campaign claims. Under the OSA, Category 1 services have a duty to protect ‘content of democratic importance’ (s 17), a systems-and-process duty that is not yet applicable and enforceable pending categorisation designation and Ofcom Codes. Taken together, the content of political advertising as such sits largely outside the OSA’s ad-specific rules considered here; hence our exclusion from scope. For an overview of the current regulation of political advertising in the UK, see House of Commons Library Briefing Paper Number 8673 on Political Advertising (1 November 2019) <<https://commonslibrary.parliament.uk/research-briefings/CBP-8673/>> accessed 28 November 2025.

²⁷On the legal architecture and limits of UK ad-recognition duties for influencers under the CAP Code and the compliance frictions these create, see Alexandros Antoniou, ‘Navigating freezones in the influencerdom: a shadowlands guide’ (2024) 29(1) *Communications Law - Journal of Computer, Media and Telecommunications Law* 8.

²⁸ASA News, ‘Putting Influencers on Notice after Monitoring Sweep Reveals Widespread Failure to Disclose Advertising’ (ASA, 18 March 2021) <www.asa.org.uk/news/putting-influencers-on-notice-after-monitoring-sweep-reveals-widespread-failure-to-disclose-advertising.html> accessed 20 June 2025; for the full report, see ASA, *Influencer ad disclosure on social media: a report into influencers’ rate of*

the ASA introduced in June 2021 a dedicated webpage to ‘name and shame’ influencers ‘routinely failing’²⁹ to comply with advertising rules regarding disclosing marketing intent. It started taking out social media ads to alert users to specific non-compliant influencers. Following an investigation by the CMA in 2018,³⁰ which also demonstrated the problems in this area, the CMA, ASA and Ofcom jointly published three sets of guidance in 2022 for social media companies, brands and influencers respectively to tackle ‘hidden advertising’.³¹ The ASA followed up with a third edition of its influencer guidance in 2023.³² A further monitoring report, published in May 2025, indicated modest improvement (with disclosure rates among previously monitored accounts rising from 35% in 2021–49%) but the ASA warned that overall disclosure levels still fell short of regulatory expectations.³³ However, due to a change in methodology (from manual monitoring in 2021 to automated data science techniques in 2024), the figures are not directly comparable, and the 2024 findings do not capture the entire influencer sector. Despite these efforts, effective enforcement or encouraging compliance in this context has proved difficult,³⁴ particularly as the rapid growth of short-form audio-visual formats has made it even easier for promotional content to blend seamlessly and appear increasingly organic. Notably, the 2025 report also confirmed that compliance rates remained lowest among the group of influencers previously subject to complaints, suggesting that targeted enforcement, while necessary, is ineffective in the face of deliberate non-compliance. It remains uncertain whether this persistent non-compliance reflects the behaviour of a relatively small but prolific cohort of repeat ‘offenders’ or a more systemic issue arising from the distinct features of the online influencer culture, particularly the fast-cycling content formats and low barriers to entry, which make widespread non-compliance difficult to track and address.³⁵ Either way, the current regime, which was essentially

compliance of ad disclosure on Instagram (18 March 2021) <www.asa.org.uk/resource/influencer-monitoring-report-march-2021.html> accessed 24 June 2025.

²⁹ASA, ‘Non-Compliant Social Media Influencers’ <www.asa.org.uk/codes-and-rulings/non-compliant-social-media-influencers.html> accessed 2 July 2025.

³⁰Competition and Markets Authority, *Social Media Endorsements* (16 August 2018) <www.gov.uk/cma-cases/social-media-endorsements> accessed 2 July 2025.

³¹Competition and Markets Authority, *Social media users set to benefit from new hidden advertising protections* (3 November 2022) <www.gov.uk/government/news/social-media-users-set-to-benefit-from-new-hidden-advertising-protections> accessed 1 July 2025.

³²ASA, *Influencers’ Guide to Making Clear that Ads are Ads* (3rd edn, 23 March 2023) <www.asa.org.uk/resource/influencers-guide.html> accessed 2 July 2025.

³³ASA, *Influencer Ad Disclosure on Social Media: Instagram and TikTok 2024* (9 May 2025) <www.asa.org.uk/resource/influencer-ad-disclosure-on-social-media-instagram-and-tiktok-2024.html> accessed 28 June 2025.

³⁴Alexandros Antoniou, ‘When likes Go Rogue: Advertising Standards and the Malpractice of Unruly Social Media Influencers’ (2024) 16(1) *Journal of Media Law* 74.

³⁵There is emerging but inconclusive market-monitoring work on disclosure failures by influencers; findings are heterogeneous and methodologically uneven. A fuller causal account is outside scope. Our focus here is doctrinal: under the CAP Code, ASA practice and intersecting consumer-protection rules, persistent non-disclosure is actionable regardless of whether non-compliance is concentrated

based on implicit acceptance of industry compliance, seems no longer fit for purpose in this distinctively online context.

Scam adverts have been a particular, persistent concern and were specifically identified by the 2017 Internet Safety Strategy Green Paper,³⁶ and recent research by the UK Safer Internet Centre shows that under-18s are exposed to them.³⁷ Some online paid-for adverts link through fraudulent content often featuring fake celebrity endorsements³⁸ or fabricated stories (see e.g. Martin Lewis/ Money Saving Expert).³⁹ In one instance, paid-for ads featured fake nudes of BBC presenter Naga Munchetty.⁴⁰ *The Guardian* also reported on scammers operating at scale using fake celebrity ads, with illicit gains totalling £27 million.⁴¹ While victims were targeted globally, about 45% were UK-based. Which? – the UK consumer advocacy organisation (Consumers' Association) – suggests that four common types of scam ads are: fake celebrity endorsements (e.g. sophisticated synthetic media featuring the likeness of celebrities such as consumer finance specialist Martin Lewis to promote fraudulent products like trading apps simulating market conditions that do not exist); AI-generated deepfakes (e.g. fabricated videos of public figures appearing to endorse scams); travel scams impersonating legitimate companies with unrealistically low prices (e.g. fake airline websites offering non-existent holiday deals); and fraudulent brand sales exploiting established reputations (e.g. fake ads promoting giveaway-style offers and directing users to deceptive sites harvesting payment details).⁴² Other patterns have emerged around event-driven schemes (e.g. scam ads

among repeat actors or reflects wider cultural dynamics. For platform-level duties and the OSA's treatment of advertising, see the discussion under 'The Online Safety Act 2023' and, in particular, 'Identifying the boundary between the general rules and Chapter 5 rules' later.

³⁶HM Government, *Internet Safety Strategy Green Paper* (October 2017) <https://assets.publishing.service.gov.uk/media/5a8222f2e5274a2e8ab57aed/Internet_Safety_Strategy_green_paper.pdf> accessed 27 June 2025.

³⁷Becca Cawthorne, 'Almost Half of 8 to 17-Year-Olds have been Scammed Online' (UK Safer Internet Centre, 11 February 2025) <<https://saferinternet.org.uk/blog/almost-half-of-8-to-17-year-olds-have-been-scammed-online>> accessed 26 June 2025.

³⁸Joe Tidy, 'Martin Lewis and Sir Richard Branson's Names Most Used by Scammers' *BBC News* (10 May 2021) <www.bbc.co.uk/news/technology-57051546> accessed 2 July 2025.

³⁹Vicky Shaw, 'Martin Lewis Issues Warning Over the Most Common Celebrity Scams' *Independent* (10 July 2024) www.independent.co.uk/news/uk/home-news/martin-lewis-scam-taylor-swift-b2577148.html accessed 2 July 2025.

⁴⁰Naga Munchetty, 'Scammers Spread Fake Nude Pictures of Me on Social Media' *BBC News* (5 February 2025) <www.bbc.co.uk/news/articles/c1ezq8ll792o> accessed 2 July 2025.

⁴¹Simon Goodley, Zoe Wood, Pamela Duncan and Michael Goodier, 'The Scammers Who Conned Savers Out of \$35m using Fake Celebrity Ads' *The Guardian* (5 March 2025) <www.theguardian.com/money/2025/mar/05/revealed-the-scammers-who-conned-savers-out-of-35m-using-fake-celebrity-ads> accessed 2 July 2025.

⁴²Which?, 'UK's Advertising Watchdog Reveals the Biggest Scam Ad Trends of 2024' (13 February 2025) <www.which.co.uk/news/article/uks-advertising-watchdog-reveals-the-biggest-scam-ad-trends-of-2024-a5GOf9b9jdud> accessed 2 July 2025. Romance scams are also problematic but do not tend to be associated with advertising; see Chiara Cavaglieri, 'Romance fraud hit £99.4m in 2024: here are 7 signs you're dating a scammer' (*Which?*, 13 February 2025) <www.which.co.uk/news/article/romance-fraud-hit-99.4m-in-2024-here-are-7-signs-youre-dating-a-scammer-avu9z2G7yuCh> accessed 24 July 2025.

offering products at heavily discounted prices on social media following Wilko's collapse),⁴³ or crisis-exploitation tactics targeting struggling consumers' fears (e.g. fraudulent ads for 'mini-heaters' that capitalised on the cost-of-living crisis).⁴⁴ In its OAP consultation, the Department for Culture, Media and Sport noted that many larger platforms offer 'self-service' advertising buying services, where there is little vetting for advertisers:

As a result, bad actors often operate with relative impunity, using online advertising as a means to perpetrate fraud or advertise other illegal or legal but harmful products and services, with limited oversight.⁴⁵

The trend towards platform-led automation may be compounding these oversight gaps. Meta, for instance, reportedly aims to fully automate ad creation and targeting via AI by 2026,⁴⁶ further streamlining the 'self-service' model but raising fresh accountability concerns.

The ASA (working with the Internet Advertising Bureau) launched in June 2020 a Scam Ad Alert service,⁴⁷ allowing users to report fraudulent ads to the ASA. Once submitted, these reports are shared with organisations participating in this scheme, including Google; Meta (Facebook/ Instagram); Taboola; Outbrain; Microsoft; TikTok; Yahoo; Snap; Twitter; Amazon Ads; Sizmek Ad Suite; RevContent; Index Exchange; Clean.io; Reach; and the Media Trust. Ads and accounts may be taken down and added to a blocklist by participating services. Platforms' response rate to notifications from the ASA are far from swift: the advertising authority reported in February 2025 that platforms responded to alerts within 48 h in 71% of cases, while 16% received responses beyond this time-frame, and 13% went unanswered.⁴⁸ Moreover, there seems to be no mechanism for ads reported directly to the platform to be fed into this system for action. Reports to

⁴³Sarah Butler, 'Scam Websites Lure in Wilko Customers with Offers Such as £4.99 Sofa' *The Guardian* (21 August 2023) <www.theguardian.com/money/2023/aug/21/scam-websites-lure-in-wilko-customers-with-offers-such-as-499-sofa> accessed 2 July 2025.

⁴⁴ASA, *Enforcement Notice Electric Plug In Mini Heaters* (9 March 2023) <www.asa.org.uk/resource/enforcement-notice-electric-plug-in-mini-heaters.html> accessed 1 July 2025. For an overview of literature examining how online financial disinformation can facilitate fraud and its impact on victims, see Ofcom, *Understanding Online Financial Harm: A Review of Fraud and Disinformation Exposure Across Demographic Groups in the UK* (27 November 2025) <www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/structure-and-leadership/online-information-advisory-committee/understanding-online-financial-harm-ofcom-literature-review.pdf?v=408230> accessed 27 November 2025.

⁴⁵Department of Culture, Media and Sport, *Online Advertising Programme Consultation* (n 16).

⁴⁶Meta aims to fully automate advertising with AI by 2026, WSJ reports' *Reuters* (2 June 2025) <www.reuters.com/business/media-telecom/meta-aims-fully-automate-advertising-with-ai-by-2026-wsj-reports-2025-06-02/> accessed 8 July 2025.

⁴⁷ASA News, 'We've Launched a Scam Ad Alert System to Help Better Protect Consumers Online' (16 June 2020) <www.asa.org.uk/news/asa-launches-scam-ad-alert-system-to-help-better-protect-consumers-online.html> 2 July 2025.

⁴⁸ASA News, 'A Year in Scams: 2024 Update on Scam Ad Alert System' (13 February 2025) <www.asa.org.uk/news/a-year-in-scams-2024-update-on-scam-ad-alert-system.html> accessed 2 July 2025.

the ASA are also shared with the National Cyber Security Centre (NCSC) to be dealt with as part of its work against phishing and scams.⁴⁹ In a separate but complementary move, Meta launched in 2025 its Fraud Intelligence Reciprocal Exchange (FIRE), enabling UK banks to share transaction intelligence directly with the platform to help detect and remove scam accounts, though its broader impact remains to be seen.⁵⁰ However, this initiative operates independently of the ASA's Scam Ad Alert system and sits in a private coordination zone that is parallel to (yet distinct from) the OSA's regulatory duties,⁵¹ underscoring the fragmented nature of current anti-fraud efforts.

The ASA requires sector-specific regulations to be respected (see e.g. the ASA's work on unregulated investments falling outside of traditional financial regulation).⁵² In addition to the ASA, some sector-specific regulators enforce advertising rules in relation to their respective areas of competence – most notably in relation to scams, the Financial Conduct Authority (FCA). In 2023, the FCA intervened to ensure the withdrawal or amendment of over 10,000 misleading financial adverts⁵³ and in 2024 launched targeted actions against so-called 'fin-fluencers' promoting financial services products illegally.⁵⁴ The FCA and ASA have a memorandum of understanding outlining their co-ordination and intersecting responsibilities.⁵⁵ However, some concerns have emerged (most recently by the Transparency Task Force) about the effectiveness of their regulatory alignment, particularly in cases

⁴⁹National Cyber Security Centre, Phishing: Spot and Report Scam Emails, Texts, Websites and Calls (26 November 2021, reviewed on 5 September 2022) <www.ncsc.gov.uk/collection/phishing-scams> accessed 1 July 2025.

⁵⁰Akila Quinio, 'Meta Expands Data Accord with UK Banks in Push to Cut Online Fraud' *Financial Times* (2 October 2024) <www.ft.com/content/ff5ed0ed-170d-4439-a789-d658936fd5f5> accessed 27 June 2025.

⁵¹Such FIRE-type arrangements operate contractually within general data-protection and sectoral-regulatory constraints: e.g., inter-firm fraud-prevention sharing is governed by UK GDPR/DPA 2018, typically relying on Article 6(1)(f) (legitimate interests in preventing crime) or Article 6(1)(c) where a specific legal obligation applies; where indicators of criminality are processed, the DPA 2018, Sch 1 para 10 (prevention or detecting of crime, 'substantial public interest') may be engaged, while Part 3 of the DPA (law enforcement processing) applies only to 'competent authorities', which most platforms and banks are not when sharing with each other. The Information Commissioner's Office (ICO) Data Sharing Code (2022) expects necessity/proportionality, data minimisation, a data-sharing agreement and a DPIA; Sch 2, para 2 (crime and taxation) may disapply certain data-subject rights, but it does not itself confer a power to share. Ofcom has no direct remit over these private exchanges under the OSA; compliance oversight sits with the ICO (data protection) and, for banks, the Financial Conduct Authority (FCA) on systems and controls; see FCA Handbook, SYSC 3 <<https://handbook.fca.org.uk/handbook/sysc3>> accessed 12 November 2025.

⁵²CAP News, 'Top Tips for Unregulated Investments' (13 February 2025) <www.asa.org.uk/news/top-tips-for-unregulated-investments.html> accessed 1 July 2025.

⁵³FCA, 'Financial Watchdog Stops Thousands of Misleading Ads and Promotions' (14 February 2024) <www.fca.org.uk/news/press-releases/financial-watchdog-stops-thousands-misleading-ads-promotions> accessed 2 July 2025.

⁵⁴FCA, 'FCA cracks down on illegal Finfluencers' (22 October 2024) <www.fca.org.uk/news/press-releases/fca-cracks-down-illegal-finfluencers> accessed 2 July 2025.

⁵⁵See *Memorandum of Understanding between the Financial Conduct Authority and the Advertising Standards Authority* <www.fca.org.uk/publication/mou/mou-fca-asa.pdf> accessed 2 July 2025.

where firms outside the FCA's perimeter engage in potentially misleading advertising.⁵⁶ The scope of the rules here is broader than ads covered by fraud offences.

Publication and dissemination of ads

While the regulation of advertising content itself remains important, the effectiveness of any regime also depends on the clarity and strength of obligations imposed on the platforms that disseminate ads. This section considers these platform-level responsibilities, beginning with the now-transitional VSP framework and moving to the more expansive model under the Online Safety Act 2023 (OSA).

The VSP regulatory model under the Communications Act 2003

Before turning to the OSA, it is instructive to recall the Video-Sharing Platform (VSP) regulatory framework under Part 4B of the Communications Act 2003.⁵⁷ We revisit it here as the immediate doctrinal precursor to the OSA's platform-side duties, and to mark what was (and was not) carried across. The VSP framework operated until 25 July 2025, when it was repealed by the OSA (Commencement No. 6) Regulations 2025;⁵⁸ from that date, VSPs became subject to the full OSA safety duties. While restricted in scope (applying to UK-established VSPs) and, in its final phase, functioning as a transitional bridge to the OSA, the VSP regime marked an early shift toward platform-level obligations in relation to advertising. Enforced by Ofcom, it imposed mandatory obligations on in-scope platforms to implement proactive measures which Ofcom's guidance made concrete: (i) advertising T&Cs were required to bar uploads for prohibited products and set conditions for restricted products (e.g. alcohol) while requiring compliance with general advertising requirements; (ii) providers were required to supply uploader functionality to declare whether a video contained advertising and make that step mandatory in the upload flow; and (iii) where the provider was aware a video contained advertising, it was required to clearly inform users (early and prominently) using a consistent identifier (e.g. an 'ad' label). These transparency duties applied to all advertising on VSPs and sat

⁵⁶Alina Khan, 'Campaign Group Calls on FCA to Act Over Firms' Advertising Practices' *Financial Times Adviser* (11 November 2024) <www.ftadviser.com/regulation/2024/11/11/campaign-group-calls-on-fca-to-act-over-firms-advertising-practices/> accessed 2 July 2025.

⁵⁷The changes to the Communications Act 2003, which transposed the 2018 revision to the Audiovisual Media Services Directive via the Audiovisual Media Services Regulations 2020 and introduced regulatory requirements for UK-established video-sharing platforms, came into effect in November 2020.

⁵⁸OSA 2023, s 210 in force since 25 July 2025 by virtue of the OSA 2023 (Commencement No. 6) Regulations 2025 (made on 17 July 2025); see also Ofcom, *Repeal of the VSP regime* (16 September 2024) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/repeal-of-the-vsp-regime> accessed 8 July 2025.

alongside additional measures for non-VSP-controlled advertising (i.e. where the advertising was not marketed, sold or arranged by the VSP), confirming the focus on provider systems and processes, not item-by-item content policing.⁵⁹

Although the VSP rules were not aimed at individual uploaders of organic videos (i.e. users) and were not explicitly designed to target scam ads, they imposed platform-level duties relevant to paid promotion. This shift from self-regulatory content rules to statutory service-design obligations marked a structural emphasis on advertising transparency and harms; it indirectly helped narrow the doctrinal space in which fraudulent, undisclosed, or misleading paid communications could plausibly circulate on VSPs by placing disclosure and enforcement on the platform's systems rather than on mere advertiser promises. However, the VSP rules did not create a free-standing duty to control where ads appear (placement controls), nor did they reach third-party programmatic pipes through a general mandate to police programmatic placement. Placement control was, at most, an indirect by-product of these system-focused provider obligations and did not extend beyond the platform's own tools and settings. Taken together, these are limited, platform-side system duties; by contrast, the ASA/ CAP regime is advertiser-facing and largely self-regulatory (with Trading Standards/ CMA backstops), relying on industry buy-in and voluntary compliance rather than enforceable placement controls. Despite calls from advocacy groups such as 5Rights urging preservation or expansion of this model within the OSA,⁶⁰ the latter's omission of analogous measures has arguably widened that space again. This gap becomes particularly salient when we turn to the persistent challenges of scam advertising.

The Online Safety Act 2023

We begin this section by offering a brief refresher of the broader online safety framework, its structure and remit, a framing necessary to understand the obligations in relation to advertisements. As discussed below, policy intent was to exclude paid-for advertising save for a confined fraud carve-in. Our analysis focuses on how that intent interacts with the enacted definitions, which (by not being adjusted in tandem) leave room for broader readings of the general duties than the policy narrative implies.

⁵⁹Ofcom, *Video-Sharing Platform Guidance: Guidance for Providers on Advertising Harms and Measures* (7 December 2021) <www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/219750-proposals-for-the-regulation-of-advertising-on-video-sharing-platforms-/associated-documents/vsp-guidance-harms-and-measures.pdf?v=327263> accessed 8 July 2025.

⁶⁰5Rights Foundation, *Ambitions for the Online Safety Bill* (April 2021) <https://5rightsfoundation.com/wp-content/uploads/2024/10/Ambitions_for_the_Online_Safety_Bill.pdf> accessed 8 July 2025.

The OSA comprises three key elements: (a) the establishment of a regulatory regime for ‘user-to-user services’⁶¹ and ‘search services’⁶² (including user-to-user services that include a search engine, e.g. Instagram’s search function) (Part 3); (b) age assurance requirements for pornography providers (Part 5); and (c) the introduction of new criminal offences, including a false communications offence.⁶³ The Act aims to reduce online harms linked to user-to-user (U2U) services, essentially, social media (and video-sharing platforms as an online platform sub-set) where users create and share content or interact with each other, and search services that allow users to search more than one website and/ or database, by imposing ‘duties of care’. At its core, it creates a risk-based regime that imposes distinct obligations pertaining to the systems and processes employed by providers to run their services and deliver content to users, particularly concerning illegal content and content harmful to children (when their services are likely to be accessed by children). Where harm arises from such content and/ or the operation of their service, they must implement effective and proportionate risk mitigation plans. Additional obligations are imposed on certain categories of services designated Category 1 (for U2U services) and Category 2A (search services), with the additional duties for Category 1 being more far-reaching than those for Category 2A.

The Act’s risk management regime varies according to the provider’s categorisation, split into three different types: (a) U2U platforms that are of significant size or functionality (Category 1);⁶⁴ (b) large search engines (Category 2A); and (c) other U2U platforms passing a size threshold (Category 2B). Ofcom serves as the independent regulator, with powers to sanction rule breakers.⁶⁵ It is a framework regime that requires secondary legislation to be enacted and the development of Guidance and Codes of Practice by Ofcom.⁶⁶ Broadcast and print media that are already regulated or self-regulated are not in scope.⁶⁷

⁶¹OSA 2023, s 3(1).

⁶²ibid, s 3(4).

⁶³ibid, s 179; for an overview of the newly introduced criminal offences, see Alexandros Antoniou, ‘New communications offences enacted by the Online Safety Act 2023’ (2024) (4) IRIS - Legal Observations of the European Audiovisual Observatory 32.

⁶⁴OSA 2023, Sch 11, para 1.

⁶⁵ibid, Part 7, Ch 6.

⁶⁶ibid, Part 3, Ch 6. For a brief overview of the Act’s structure, categorisation logic and staged implementation, see Hedvig Schmidt, ‘The Online Safety Act 2023’ (2024) 16 Journal of Media Law 202.

⁶⁷Under the 2003 Communications Act, Ofcom is required to implement procedures for handling and resolving complaints from listeners and viewers about programmes broadcast on radio and TV channels that it licences; see Ofcom, *Procedures for handling complaints, investigations and sanctions on TV, radio and video-on-demand services* (12 January 2016, updated on 23 June 2025) <www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-standards/procedures> accessed 8 July 2025. This includes the Welsh channel, S4C and Ofcom’s enforcement role also extends to the BBC. Ipso and Impress are the two press regulators in the UK. Both are voluntary, and not all news publications are members of them; see further John Woodhouse, *How is the press regulated?* (Research Briefing Number 7576, House of Commons Library, 16 July 2024) <<https://researchbriefings.files.parliament.uk/documents/>

Despite advertising's centrality to the online experience, and its capacity to expose users to harms, it was not integrated into the OSA's initial design. This omission sharpened attention on the adequacy of existing regulatory tools, particularly the efforts of the ASA and CMA. The ASA and the CMA's targeting of social media platforms and other online intermediaries was far from comprehensive, so the government recognised the need for a more coordinated approach.⁶⁸ Yet, the initial draft version of the Online Safety Bill (and by contrast to the VSP rules) excluded advertising: specifically, its clause 39(2) expressly excluded 'paid-for advertisements'.⁶⁹ This took out of the regime the content of ads delivered by regulated services with a further sub-clause describing paid-for ads as those where the payment goes to the delivery system.⁷⁰ Arrangements where the payment would go to the content producer would therefore *not* have been excluded and thus, influencer marketing content would have been relevant content for the draft Bill. A similar approach could be seen in relation to search services, whereby 'search results' did not include paid-for advertisements.⁷¹ Even though influencer content was caught by the draft Bill, fraud offences were not listed as priority offences triggering the regime.

Following a successful campaign by consumer groups, financial sector organisations and mental health charities,⁷² and in response to Parliamentary concerns raised during the pre-legislative scrutiny of the draft Bill,⁷³ the government confirmed it would include fraudulent 'paid-for advertisements' in the regime. It added a discrete set of duties (Chapter 5 of Part 3 to the OSA; hereafter 'Chapter 5 duties', referring to Part 3, unless otherwise stated) and adjusted some of the main definitions accordingly.⁷⁴ Fraud offences were included in Schedule 7 as priority offences triggering the generally applicable duties; influencers remained within the scope of these duties. As we demonstrate below, while the policy intent seemed to aim

[CBP-7576/CBP-7576.pdf](#)> accessed 8 July 2025. Strictly, the OSA carves out 'news publisher content' and defines 'recognised news publishers' (ss 55–56). These categories (covering, inter alia, the BBC, S4C, licensed broadcasters and entities meeting the statutory criteria) map onto the familiar 'broadcast/ print' shorthand used here. For an analysis of the relevant OSA provisions, see Ricki-Lee Gerbrandt, 'Threatening & protecting press publishers and journalism in the UK's regulation of social media platforms' (2025) 17 *Journal of Media Law* 68.

⁶⁸Department of Culture, Media and Sport, *Online Advertising Programme Consultation*, Section 3: Harms caused by online advertising (n 16).

⁶⁹Draft Online Safety Bill (CP 405), cl 39(2)(f).

⁷⁰*ibid*, cl 39(7).

⁷¹*ibid*, cl 134(5).

⁷²Anabel Hoults, 'Win! Scam Ads Included in the Online Safety Bill' *Which?* (9 March 2022) <www.which.co.uk/news/article/win-scam-ads-included-in-the-online-safety-bill-from-anabel-hoults-which-chief-executive-aT4Gc9V7rXJ9> accessed 29 June 2025.

⁷³Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill* (2021–22, HL 129, HC 609) 75–78.

⁷⁴Department for Digital, Culture, Media and Sport, Home Office et al, 'Major Law changes to Protect People from Scam Adverts Online' (8 March 2022) <www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online> accessed 2 July 2025.

generally to exclude platform- and search-delivered ads from the regime apart from these new specific rules, this series of changes has introduced some ambiguity into the scope of the OSA regime overall. This set of changes would not, however, cover the open display market but only the ‘walled garden’ environments provided by regulated U2U and search services under the OSA.

How the OSA regulates ads (Chapter 5 rules: fraudulent ads)

The fraudulent ads provisions are found in Chapter 5 of Part 3 of the OSA. It imposes two pillars on in-scope services: (a) operational duties that focus on preventing and managing the presence of fraudulent ads (particularly through preventative measures, minimisation of exposure and responsive action; more on these below); and (b) transparency duties to disclose any proactive technologies employed for compliance. However, these are not uniform. The respective duties for U2U and search services differ slightly to account for the distinct nature of each service. The following paragraphs set out these two pillars and their divergences for U2U and search services.

More specifically, the Chapter 5 duties require **Category 1** (U2U) to operate their service using proportionate systems and processes to:

- i prevent individuals from encountering fraudulent ads;⁷⁵ this could include, for example, a fake investment scheme ad displayed and viewed in a user’s feed but would not include any subsequent interactions with the ad’s destination page (e.g. where the user clicks the ad and lands on a fraudulent website), as the focus appears to be solely on the initial presentation of the ad, not on what happens after the user engages further with the ad’s content;⁷⁶
- ii minimise the length of time such ads are present;⁷⁷ and
- iii swiftly remove them once they obtain knowledge of them through any means⁷⁸ (e.g. where they identify it or have been alerted to their presence).

In addition to these operational duties, under the second pillar, Category 1 service providers have a transparency obligation, namely to detail in their terms of service (ToS) clearly and accessibly any proactive technology used to address fraudulent advertising, including information on the nature, usage and functionality of such technology.⁷⁹ The factors for determining what is proportionate in relation to providers’ systems and processes to

⁷⁵For the meaning of ‘encountering’, see s 236(1): ‘[...] read, view, hear or otherwise experience content’.

⁷⁶OSA 2023, ss 38(1)(a) and 38(6).

⁷⁷ibid, s 38(1)(b).

⁷⁸ibid, s 38(1)(c).

⁷⁹ibid, s 38(2).

comply with their fraudulent ad duties include: (i) the nature and severity of potential harm posed by different kinds of ads, and (ii) a provider's degree of control in relation to the ads' placement on the service.⁸⁰

Similar to Category 1 providers, the fraudulent ads prevention and mitigation duty for **Category 2a** (search) services involves obligations to:

- i prevent individuals from encountering fraudulent advertisements in or via search results;⁸¹
- ii minimise the duration of time that fraudulent ads are encountered if they appear;⁸² and
- iii act swiftly to remove fraudulent advertisements upon being alerted or becoming aware of their presence.⁸³

References to 'encountering'⁸⁴ fraud ads in the case of search providers extend to interacting with paid-for ads in (or via) search results.⁸⁵ The approach here covers *both* the ad's initial display in search results *and* the immediate consequences of user interactions with it, emphasising a responsibility to manage and prevent fraudulent ads right from the search results page. So, in statutory terms, search 'encountering' captures the click-through from those results ('via'), but U2U 'encountering' is confined to presentation on the service.⁸⁶ For example, if a user searches for 'best investment opportunities' on a search engine and clicks on a paid-for ad about a limited-time offer of a bogus crypto scheme, that click-through from the results page, i.e. the paid result is displayed, and the user is immediately redirected to a website promoting a fraudulent cryptocurrency investment, constitutes the 'encounter' for the purposes of the Act.⁸⁷ Thus, the duty for search attaches to the initial display and immediate redirection from the results page. Further interactions, e.g. subsequently navigating the linked website, or signing up and filling out forms on the destination site

⁸⁰ *ibid*, s 38(5).

⁸¹ *ibid*, s 39(1)(a).

⁸² *ibid*, s 39(1)(b).

⁸³ *ibid*, s 39(1)(c).

⁸⁴ *ibid*, s 236 and (n 74).

⁸⁵ *ibid*, s 39(4).

⁸⁶ *ibid*, s 39(4) provides that references to encountering fraudulent advertisements 'in or via search results' include interacting with a paid-for ad in those results but do not extend to subsequent interactions on the destination site. By contrast, the Category 1 duty uses 'by means of the service' under s 38(1)(a) with no equivalent extension.

⁸⁷ *ibid*, Explanatory Notes, para. 237. Ofcom has described search engines as 'one-click gateways' to harmful content in research and communications around illegal/ harmful content (self-injury, eating disorders). We cite this as evidence of likely operational/ enforcement focus (not as a general legal principle limiting s 39). The statutory phrase 'in or via search results' remains the legal anchor; see e.g., Ofcom, 'Search engines can act as one-click gateways to self-harm and suicide content' (31 January 2024) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/search-engines-one-click-gateways-to-self-harm-content> accessed 5 December 2025.

falls outside the search ‘encounter’, while U2U ‘encountering’ remains limited to content presented within the U2U service.

For Category 2a services too (under the second pillar), there is a transparency obligation in (and accountability for) the technology used: search services must disclose in a publicly available statement any proactive technology and the methods used to enforce the above-mentioned preventative and corrective actions,⁸⁸ e.g. through a dedicated section on the company’s website outlining anti-fraud software or monitoring systems.

Similar to U2U, proportionality regarding search services’ systems and processes for handling fraudulent ads is assessed by looking at the nature, severity and potential harm posed by such ads, along with the service providers’ degree of control over placements (considering direct management versus reliance on third-party networks).⁸⁹ So, a small aggregator search engine that relies on external ad sources and has limited control over ad placements would need to adjust its approach based on its capacity. A niche engine that compares financial products (e.g. loans and investment accounts) and relies on ads from external sources may have less direct control over ad placements, but the potential for harm remains serious (even if not on the scale of larger platforms). A tailored, balanced response could involve implementing robust monitoring systems and acting promptly on alerts from trusted partners, or user reports, rather than building in-house sophisticated algorithms.

The Chapter 5 duties are triggered only by adverts that relate to certain fraud crimes listed in s 40 of the OSA. The specified offences broadly comprise: financial services misconduct (i.e. unauthorised or unexempted financial activities, false claims of authorisation or exemption and breaches of financial promotion restrictions in violation of the Financial Services and Markets Act 2000); fraudulent activities (i.e. fraud by false representation or abuse of position, making or supplying articles for use in fraud and participation in fraudulent business operations in breach of the Fraud Act 2006); misleading information (i.e. making misleading statements and creating misleading impressions in contravention of the Financial Services Act 2012); and finally, attempts and complicity (i.e. the relevant inchoate offences also apply to the definition of fraud offences). This is a much narrower list of offences than those covered by the general illegal content

⁸⁸ibid, s 39(2).

⁸⁹ibid, s 39(6). For the avoidance of doubt, this proportionality enquiry is anchored in s 39(6) itself (i.e., how harmful the ads could be, and how much control the service really has over where ads appear) and is not created by the Act’s search risk assessment duties. The s 26 (illegal content) and, where relevant, s 28 (children’s) risk assessments run in parallel and (per the Act and its Explanatory Notes) inform duties under s 27/ 29; Chapter 5 does not add a separate statutory risk assessment duty. Providers may cross-refer their s 26/ 28 assessments to support and justify the systems and processes adopted under s 39, but those assessments are evidential scaffolding to justify their approach, not the legal test under s 39(6).

duties.⁹⁰ The Chapter 5 narrowing is not because other illegal content offences are irrelevant to advertising. Many plainly are, e.g. offences in Schedules 5–7 (priority offences) relating to child sexual abuse material, prohibited weapons, or controlled drugs. Rather, Parliament ring-fenced Chapter 5 to the ‘fraud etc.’ offences in s 40 as a targeted carve-out.

This narrowing leaves a significant gap in the regime in relation to adverts: on a strict reading of the OSA as presently administered, when paid-for advertising itself promotes, distributes, solicits, or links to CSAM, Chapter 5 does not bite (it is tied to s 40 ‘fraud etc’ offences), and the general Part 3 duties either do not reach paid-for ads in search,⁹¹ or for U2U depend on whether such ads are ‘user-generated content’, a contested and unresolved point we analyse below (see ‘Identifying the boundary between the general rules and Chapter 5 rules’). Thus, because Chapter 5 is confined to s 40 fraud, non-fraud illegal adverts (including CSAM for example) have no Chapter 5 duty hook. For search services, paid-for ads are outside the general Part 3 illegal content duties by definition; for U2U, the general duties apply only if paid ads count as ‘user-generated content’ (addressed later). If paid-for ads are not user-generated content, no Part 3 duty compels *ex ante* or *ex post* measures against CSAM in paid placements. That is the significance: the narrowing in Chapter 5 makes resolution of the general duties question dispositive for whether the OSA reaches illegal ad content beyond fraud.

The Chapter 5 duties are imposed only on a subcategory of U2U and search services respectively: Category 1 and Category 2a. However, although relevant regulations to start the categorisation process have recently come into force,⁹² we do not know exactly which services will be caught – and so the rules remain unenforceable for now. Uncertainty around categorisation briefly spiked when the Wikimedia Foundation issued judicial review proceedings against the government’s Categorisation Regulations.⁹³ In August 2025, the High Court dismissed the challenge, holding the Regulations lawful.⁹⁴ The Court, however, indicated that Wikimedia (or any provider) could challenge Ofcom’s eventual designation decisions if, after

⁹⁰*ibid.*, ss 10, 27.

⁹¹OSA 2023, ss 55(2) and 57(2)(a) and definition of ‘paid-for advertising’ in s 236.

⁹²The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regs 2025.

⁹³Wikimedia argued that certain thresholds, notably those linked to content recommender systems and forwarding or sharing functionality, could inadvertently endanger the safety of volunteer editors and expose the encyclopaedia to ‘manipulation and vandalism’; see further Wikimedia Foundation Policy, ‘Wikipedia’s Non-profit Host Brings Legal Challenge to New Online Safety Act (OSA) Regulations’ (8 May 2025) <<https://medium.com/wikimedia-policy/wikipedias-nonprofit-host-brings-legal-challenge-to-new-online-safety-act-osa-regulations-0f9153102f29>> accessed 7 July 2025 and Chris Vallance, ‘Wikipedia legally challenges “flawed” online safety rules’ *BBC News* (8 May 2025) <www.bbc.com/news/articles/c62j2gr8866o> accessed 7 July 2025.

⁹⁴*Wikimedia Foundation & BLN v Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin, 11 August 2025).

engagement, they consider Ofcom has misapplied the statutory scheme. Wikimedia has since confirmed it will not appeal.⁹⁵ The immediate effect is that the Categorisation Regulations remain in force as made; residual litigation risk now lies in future, provider-specific designations, not in the validity of the Regulations themselves. Generally, it seems that only large services will be caught as Category 1 or Category 2a services – a decision which was controversial given that the Act allowed for services to be included in Category 1 on the basis of risk as well as size.⁹⁶ So, scams on small services (even those aimed at children) will not be caught by the regime. Although the Categorisation Regulations are now in force in their original draft, Ofcom has not yet designated which services fall within Category 1, 2A or 2B. Accordingly, some category-contingent duties remain in abeyance pending designation and for Chapter 5 until Ofcom's Code of Practice⁹⁷ is in force,⁹⁸ which is not expected until mid-2027.⁹⁹ In late March 2025, UK Finance (a trade association for the UK banking and financial services sector) and Which? called for swifter action on fraudulent ads in a joint letter to the government.¹⁰⁰ Following the High Court's dismissal of Wikimedia's challenge and Wikimedia's decision not to appeal, the validity of the Categorisation Regulations is settled; timing now turns on Ofcom's designation decisions and the commencement of the relevant Code of Practice.¹⁰¹

Application of the Chapter 5 (OSA Part 3, Chapter 5) rules

Only those adverts (as defined under ss 38(3) and 39(3) together with s 236 of the Act) are regulated content for the purpose of the Chapter 5 duties. There are two relevant definitions: one for Category 1 services, the other for Category 2a. For ease, both definitions comprise limbs (a) and (b); the Category 1 definition only, includes an additional limb (c), detailed below.

⁹⁵Paul Sandle, 'Wikipedia will not appeal dismissal of its UK Online Safety Act challenge' *Reuters* (12 September 2025) <www.reuters.com/world/uk/wikipedia-will-not-appeal-dismissal-its-uk-online-safety-act-challenge-2025-09-12/> accessed 3 October 2025.

⁹⁶For context on the Secretary of State's decision to follow Ofcom's service categorisation, excluding smaller yet harmful platforms from Category 1 and thereby exempting them from the Act's most stringent obligations, despite strong opposition from mental health, suicide prevention, and anti-hate advocacy groups, see Online Safety Act Network, *Categorisation of services: next steps* (17 December 2024) <www.onlinesafetyact.net/analysis/categorisation-of-services-next-steps/> accessed 2 July 2025.

⁹⁷OSA 2023, s 41(4).

⁹⁸*ibid*, s 51(7).

⁹⁹Ofcom's approach to implementing the Online Safety Act (last updated 12 November 2025) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation> accessed 29 November 2025.

¹⁰⁰UK Finance and Which? letter to government on tackling fraud (25 March 2025) <www.ukfinance.org.uk/news-and-insight/press-release/uk-finance-and-which-letter-government-tackling-fraud> accessed 2 July 2025.

¹⁰¹See (n 99) for Ofcom's updated online-safety timetable: publication of the categorisation register and a consultation on additional duties for categorised services are expected around July 2026.

In relation to **Category 1** services, subsection 38(3) defines a ‘fraudulent advertisement’ as an advertisement that meets *all three* of the following conditions:

- a) *It is a paid-for advertisement (as defined by s 236):* Consideration is provided for its inclusion or promotion on the service and the placement is determined by systems or processes (rather than appearing naturally or for free) agreed under the advertising arrangement (including via intermediaries).¹⁰²
- b) *It amounts to an offence specified in s 40:* The advertisement’s content is illegal because it falls under the types of criminal fraud offences listed in s 40.
- c) *It is not regulated user-generated content:* The content must be an advertisement in its own right, i.e. created and distributed through paid advertising rather than posted directly by users.

In summary, for the purposes of Category 1 duties, an advert qualifies as ‘fraudulent’ if it is paid-for and linked to a s 40-listed criminal offence that is not user-generated content under the Act. An illustrative example engaging, for instance, s 2 of the Fraud Act 2006 (fraud by false representation, a s 40 listed offence) could involve an ad for a cryptocurrency platform claiming a 20% monthly return (allegedly backed by multiple investors), while featuring manipulated graphs that suggest substantial profit gains. In this scenario, the platform could either receive direct payment from the scammer for running the ad or instead, acquire free access to the scammer’s network and analytics tools which could assist in tracking user engagement and boosting its ad revenue. The ad’s placement (which presumably includes position and frequency on users’ feeds) is driven by the platform’s algorithm, targeting users based on interests or search history (e.g. users interested in financial topics or quick financial gains), as per the advertising agreement.

In relation to **Category 2a** services, subsection 39(3) defines a ‘fraudulent advertisement’ as an advertisement that meets both of the following conditions:

- a) *It is a paid-for advertisement (as defined by s 236):* Consideration is provided for its inclusion or promotion on the service (e.g. a financial transaction to be displayed on the search service) and the placement is determined by systems or processes agreed under the advertising arrangement (including via intermediaries).¹⁰³
- b) *It amounts to an offence specified in s 40:* The advertisement’s content is illegal because it falls under the types of criminal fraud offences listed in s 40.

¹⁰²For both Category 1 and Category 2A, the OSA uses the *same* definition of ‘paid-for advertisement’; see ss 38(3)(a) and 39(3)(a) each cross-referring to s 236.

¹⁰³*ibid.*

Thus, for the purposes of Category 2a duties, an advert qualifies as ‘fraudulent’ if it is both paid-for and its content amounts to a s 40-listed offence.

As well as introducing these provisions, the revisions also removed the exclusion of paid-for ads in relation to U2U services but left it intact for search services.¹⁰⁴ The implications of this are not clear, as we illustrate below.

Identifying the boundary between the general rules and Chapter 5 rules

The key point of distinction between the general Part 3 duties and the Chapter 5 duties seems to be the fact that the definition of an advert for the purposes of the specific fraudulent ad duties *excludes* ‘user-generated content’.¹⁰⁵ This suggests that the general duties would apply to what has been termed ‘organic content’ (i.e. content appearing without paid placement and which could include some commercial messaging in posts, product placement and the like) produced by ‘users’ but *not* messages distributed through paid systems fed into the system by advertisers, which would be caught by the Chapter 5 rules instead.

This interpretation depends on the meaning given to ‘user-generated content’. The term is defined in s 55(3) and has two core elements:

- (a) being ‘generated directly’, ‘uploaded to’ or ‘shared on’ the service; and
- (b) being capable of being encountered by other users.

This aligns with the definition of a U2U service in s 3(1) of the OSA which contains the same two elements. The *second* core element is non-problematic: advertisements are inherently intended for user visibility. The *first* element requires the (direct) supply of the material to the service, which presumably happens when the advertiser places the advert for delivery. So, the question is whether the service referred to is the same one for advertisers and other users. The text does not provide a clear answer, but non-advertiser users encounter organic posts and advertising simultaneously within the same interface – from their perspective there is one service, supplying both forms of content, i.e. organic and advertising content together. This is the hinge: if the advertiser is using the same service interface as ordinary users, a broader reading of the provisions is textually available; if not, a narrower, policy-consistent reading governs. We now consider the implications of both below.

More specifically, there are two reasonable readings of the relevant definitions as they apply to advertising: (a) a narrow, consistent with the policy intent reading under which paid-for ads are not ‘user-generated content’ and advertisers are not treated as ‘users’ for Part 3; and (b) a

¹⁰⁴OSA 2023, ss 55(2) and 57(2)(a) and definition of ‘paid-for advertising’ in s 236.

¹⁰⁵*ibid*, s 38(3)(c).

more expansive, text-led reading under which advertisers can be ‘users’ for s 55(3), bringing some paid-for ads within the general Part 3 duties for U2U services (search remains limited by the Act’s exclusion of paid-for ads from the definition of ‘search content’).¹⁰⁶

Reading A (narrow, policy-consistent): one possibility is that ad delivery clients are *not* considered ‘users’ of regulated services when they buy paid placements, and consequently their paid-for content is not classified as ‘user-generated’ and thus outside the general Part 3 U2U rules (only Chapter 5 applies where s 40 offences are made out). This interpretation would match the policy intent noted above (see the discussion under ‘The Online Safety Act’ earlier).

However, the definition of ‘user’¹⁰⁷ (Figure 1), which underpins ‘user-generated content’,¹⁰⁸ does not seem necessarily to exclude advertisers from being considered users. Specifically, s 227 excludes those acting ‘in the course of the provider’s business’ (owners/ managers, employees, volunteers, consultants). It does not carve out advertisers or agencies *as a class*. Read with s 55(3) (outlined earlier), an advertiser supplying material to the same service interface used by end-users can plausibly be a ‘user’. Likewise, the requirement that a user be in the UK is about the regime’s geographical scope, not the nature of the users. Consequently, another interpretation of the interrelationship between the general Part 3 rules and those relating to fraudulent adverts remains viable (we mark this as **Reading B**).

Reading B (broader, textually possible): If advertisers *are* considered ‘users’, more content will be dealt with under the general Part 3 rules (although not for search services; see the discussion earlier), considerably narrowing the application of the fraud-specific duties. The impact of this interpretation on fraudulent ads would not be great, given that fraud is also listed in Schedule 7 as priority content for the purposes of the general U2U duties.¹⁰⁹ Adopting Reading B would, however, mean that social media services would have duties, which came into force on 17 March 2025,¹¹⁰ to address illegal advertisements they disseminate, not only those linked to the offences outlined in s 40. So, this would potentially require action against ads for firearms, illicit drugs, and deepfake pornography. Additionally, this interpretation suggests an obligation to prevent pornographic advertisements from reaching minors; an area where recent

¹⁰⁶OSA, s 57(2)(a); see also (n 104) earlier.

¹⁰⁷*ibid*, s 227.

¹⁰⁸*ibid*, s 55(3).

¹⁰⁹Ofcom, *Protecting People from Illegal Harms Online: Illegal Content Judgements Guidance* (16 December 2024) <www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-judgements-guidance-icjg.pdf?v=387556> accessed 2 July 2025.

¹¹⁰Ofcom, ‘Enforcing the Online Safety Act: Platforms must start tackling illegal material from today’ (17 March 2025) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/enforcing-the-online-safety-act-platforms-must-start-tackling-illegal-material-from-today> accessed 1 July 2025.

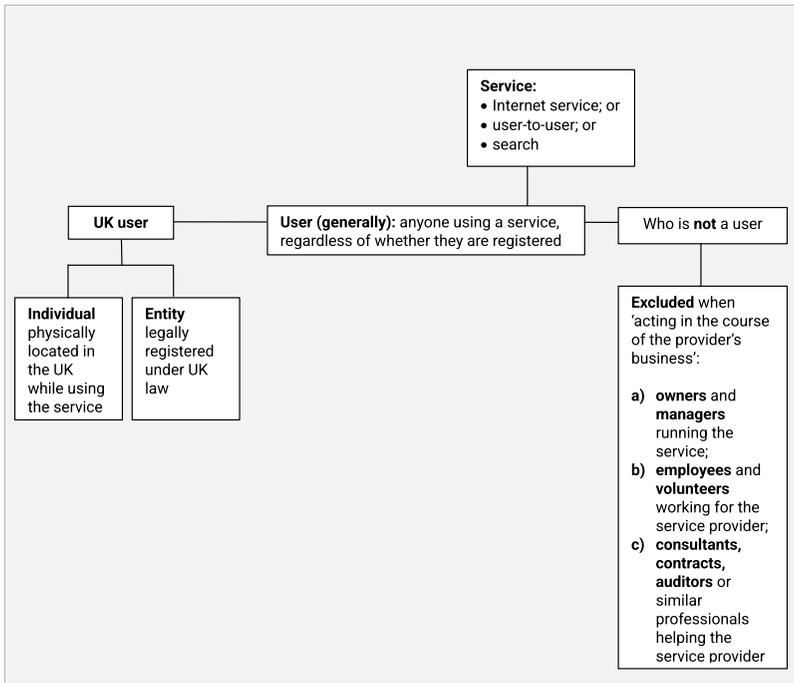


Figure 1. ‘User’ and ‘United Kingdom user’ under s 227 of the OSA. Boxes on the left show who counts as a UK user; the right box lists those excluded only when acting ‘in the course of the provider’s business.’ Advertisers (and influencers) who submit material to a service can, *prima facie*, be treated as ‘users’, unless acting in the course of the provider’s business. Source: authors’ own illustration.

research indicates significant deficiencies on the part of at least some U2U services.¹¹¹ The Reading A/ B outcomes are crystallised in [Table 1](#) below.

Ofcom’s current approach does not, however, appear to follow this interpretation, but its published materials seemingly track **Reading A** as the current regulatory baseline which is more in line with the policy intent (i.e. paid placements are outside the general Part 3 U2U rules and within Chapter 5 only where s 40 is engaged). Questions have been raised during the consultations on the general Codes. In the stakeholder response document issued as part of the illegal harms consultation, Ofcom noted:¹¹²

A1.7.7 The Global Disinformation Index wanted clarity as to whether programmatic advertising services would be within scope of these measures. It

¹¹¹AI Forensics, *Pay-to-Play: Meta’s Community (Double) Standards on Pornographic Ads* (8 January 2025) <<https://aiforensics.org/work/meta-porn-ads>> accessed 1 July 2025.

¹¹²Ofcom, *Protecting People from Illegal Harms Online - Annex 1: Further Stakeholder Responses to Our November 2023 ILLEGAL Harms Consultation* (16 December 2024) 68 <www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/annex-1--further-stakeholder-responses.pdf?v=388774> accessed 27 June 2025.

Table 1. Who is a ‘user’ under s 227 OSA in the advertising context, and what follows.

Actor	Counts as ‘user’ under s 227	UK-user test	Consequence for ad material	Statutory (OSA) provision
Ordinary user posting content	Yes	Present in UK while using	Their ad-like post can be ‘user-generated content’; general Part 3 duties may apply (plus Sch 7 priority offences; children’s duties where relevant)	ss 3(1), 55(2), Sch 7
Influencer posting own promotional content (not a paid placement)	Yes	As above	Treated as ‘user-generated content’; general Part 3 duties (U2U) apply	ss 3(1), 55(3)
Advertiser purchasing a paid-for placement on a U2U service	Yes, in principle (not acting in the course of the provider’s business)	UK presence or UK entity	Two readings: Reading A (narrow, policy-aligned), not user-generated; only Ch 5 applies if s 40 offence. Reading B (broader, textually plausible): may <i>still</i> be user-generated; general Part 3 duties can bite – unsettled .	ss 55(3), 227, 38-40, Sch 7
Media/ creative agency uploading on advertiser’s behalf	Same as advertiser (agency is <i>not</i> the service provider)	UK presence or UK entity	Same consequences as row above	s 227
Platform owners, managers, employees, volunteers, consultants while acting for the provider	Excluded (‘in the course of the provider’s business’)	N/A	Their uploads are not ‘user-generated content’; duties arise via systems/ process obligations, not via ‘user’ status.	s 227(3)-(7)
Search service paid-for placement	‘User’ status not determinative ^a	As above	General Part 3 search duties exclude paid-for ads; Chapter 5 applies only where s 40 offence and ‘encounter in or via’ search results.	ss 57(2)(a), 40

^aFor ease, general Part 3 duties for search expressly exclude paid for ads (so even if the advertiser was a ‘user’, those general duties do not bite on paid placements) and Chapter 5 on fraudulent ads for search does not turn on ‘user-generated content’ at all, as it only asks whether an item is paid-for ad that amounts to a s 40 offence and is encountered in or via search results; OSA, ss 39(3), 55(2) and 57(2)(a).

also highlighted that if these services are not captured there is potential risk that it does not report data that could reveal the extent to which illegal content is being funded and amplified on services.

Our response:

A1.7.8 The Act sets out the services that are in scope of the online safety regime. If a person provides an online service, it may be in scope of these duties. It is up to the provider to assess the nature of their service and, if

necessary, seek independent specialist advice to determine whether or not their service would be subject to the requirements of the Act.

This somewhat ambiguous response could be understood against a more recent elaboration in relation to its Code on Content Harmful to Children (Vol 2).¹¹³ Following concerns expressed by some respondents to the consultation about ‘surveillance advertising’, Ofcom commented:¹¹⁴

5. 49: [...] We emphasise that all service providers must consider their revenue model in their children’s risk assessments, as it is a general risk factor in the Children’s Risk Profiles. The Children’s Register details how revenue models, such as advertising to generate income, can create financial incentives that may lead businesses to expose children to harmful content. For instance, if harmful content is engaging, service providers may have a financial incentive to recommend such content to children in order to generate more revenue from advertising. Therefore, if a service provider uses ‘surveillance advertising’, it must consider the impact this has on children encountering harmful content on their service. However, it is beyond our powers under the Act to ban this form of advertising.

This suggests that where adverts (incl. those targeting children) are linked to illegal or harmful content, then a provider’s business model and delivery system (e.g. placement mechanisms) should be considered relevant factors for risk assessment and associated safety duties under Part 3. However, the presence of criminal or harmful adverts does not by itself trigger Chapter 5; those duties arise only for paid-for ads amounting to s 40 ‘fraud etc.’ offences. Doctrinally, this matters because the general Part 3 duties (now in force for illegal content) can require system-level mitigations on U2U services, whereas Chapter 5 is narrower and not yet enforceable. Non-content concerns about the targeted delivery of adverts that determine which users see ads (e.g. default placement settings, bidding parameters) would likewise not independently trigger the regime.

The inclusion of adverts in the regime implies that the business systems for accepting ad copy and delivery/ publishing the ads (insofar as it is operated by the provider as part of the service) would be included in the safety obligations. This would seem to be true as regards the specific fraudulent ad rules and – potentially – the general Part 3 rules, though the impact on those systems for general Part 3 rules purposes might seem more indirect than for the fraudulent ad rules. Moreover, external delivery services and other actions in the online advertising environment would escape this net, but they would still need to comply with e.g. data protection rules. In

¹¹³Ofcom, *Protecting Children from Harms Online - Volume 2: The Causes and Impacts of Online Harms to Children* (24 April 2025) 44 <www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-2-the-causes-and-impacts-of-online-harms-to-children.pdf?v=396646> accessed 2 July 2025.

¹¹⁴*ibid*, 44–45.

principle, this could mean that some problems around ad fraud remain unaddressed,¹¹⁵ despite these layered obligations.¹¹⁶

Although the government at the time aimed (see ‘The Online Safety Act 2023’ section earlier) to confine regulatory duties for paid-for ads to a narrow set of fraud-related offences, the legislation’s text leaves open broader interpretations, particularly concerning whether certain ads fall within the general Part 3 illegal content duties. Crucially, these general duties became enforceable in March 2025,¹¹⁷ whereas Chapter 5 duties will not be enforceable until Ofcom’s Code of Practice takes effect, likely in 2027.¹¹⁸ The Codes may be the natural loci to settle the interpretive choice mapped here. If a broader reading of ‘user-generated content’ and ‘user’ prevails, U2U services may already be subject to wider obligations regarding illegal ads. This interpretative ambiguity allows for a divergence in enforcement expectations from what the previous government intended, potentially accelerating regulatory exposure for in-scope services before Ofcom’s ad-specific rules come into force. Our recommendation is therefore not to expand the Act but to standardise this broader, text-led construction (Reading B) – treating advertisers as potential ‘users’ for s 55(3) where their material is supplied to the same user interface – in Ofcom’s General Part 3 illegal content Codes/guidance for U2U services.¹¹⁹ A cross-reference can be included in the forthcoming Chapter 5 fraudulent-ads Code (and accompanying guidance) for coherence. This would not purport to create new duties; it would clarify and operationalise a textually plausible construction to remove ambiguity and reduce compliance uncertainty. It would align treatment of organic and paid placements on U2U services, while preserving the statutory carve-out for search.

The Online Advertising Programme (OAP)

The OAP was intended to look at the online advertising market across the board. It is still short on delivering results. The then government formed a

¹¹⁵For an EU comparator (DSA ad-specific transparency, including VLOP ad repositories, alongside general illegal-content rules that also bite on ads, with some adtech intermediaries potentially qualifying as ‘platforms’), see Pieter Wolters, and Frederik Zuiderveen Borgesius, ‘The EU Digital Services Act: what does it mean for online advertising?’ (2025) 33 *International Journal of Law and Information Technology* <https://doi.org/10.1093/ijlit/eaaf004>.

¹¹⁶For the avoidance of doubt, wasted ad spend (referred to earlier in our introduction), by itself, does not engage the Part 3 duties: the OSA’s illegal-content and children’s-safety duties are harm-facing and user-protective. Budgetary loss to an advertiser only becomes relevant where the ad content independently falls within the illegal-content duties (for U2U) or Chapter 5’s s 40 offences (for Category 1/ 2A), or where systems and processes increasing users’ exposure to such content trigger risk-mitigation obligations.

¹¹⁷Ofcom, ‘Important Dates for Online Safety Compliance’ (17 October 2024, updated on 24 April 2025) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/important-dates-for-online-safety-compliance> accessed 4 July 2025.

¹¹⁸Ofcom’s approach to implementing the Online Safety Act (n 99); see ‘How the OSA regulates ads’ earlier.

¹¹⁹Ofcom, ‘Quick Guide to Illegal Content Codes of Practice’ (9 November 2023, updated on 4 July 2025) <www.ofcom.org.uk/online-safety/illegal-and-harmful-content/codes-of-practice> accessed 4 July 2025.

taskforce; more concretely, the Online Fraud Charter was agreed.¹²⁰ This is a set of voluntary commitments for companies to sign on to. Although a six-month review was scheduled, there is no sign of an output from that review (assuming the review even took place, given the timeline was before the 2024 General Election). One year after its implementation, Which? research indicates that the Charter has had limited success in reducing scams: despite the commitments made, fraud is ‘still rife’ on online platforms in the UK.¹²¹

The OAP taskforce released a progress report,¹²² but its focus appears to mirror that of the OSA, largely addressing content-based issues, rather than the broader advertising delivery system (despite earlier consultation concerns about ad tech and structural fraud risks). Notably, in its response to the OAP consultation, the ASA endorsed the need for reform and recognised that online advertising harms fall into multiple categories, ranging from rule breaches by bona fide advertisers (e.g. misleading claims) to illicit activity by criminal actors (e.g. scams, investment frauds, human trafficking) and systemic risks affecting the integrity of the advertising ecosystem itself (e.g. unreliable performance metrics and brand safety concerns linked to the context or placement of an otherwise compliant ad). Crucially, the ASA drew a sharp line around its own remit, which is confined to almost entirely to the first of these (i.e. those involving non-compliance by legitimate advertisers), and made clear that it lacks both the mandate and resources to address harms stemming from criminal exploitation or supply chain dysfunction.¹²³ This paints the picture of an incoherent configuration where less visible layers of the ad supply chain remain under-regulated,¹²⁴ showing the need for a more joined-up response across the broader online advertising ecosystem.

In particular, the limitation in terms of actors caught under the OSA, which essentially excludes the open advertising environment, has not been addressed by the OAP. This in parallel raises the question: if the OAP’s scope aligns with the OSA, why were ads excluded in the first place? The Labour government confirmed the OAP will continue for 12 months from December 2024 under updated terms of reference that reflect this focus.¹²⁵

¹²⁰Home Office, *Online Fraud Charter* (30 November 2023) <www.gov.uk/government/publications/online-fraud-charter-2023> accessed 1 July 2025.

¹²¹Ash Strange, ‘A Year On from the Online Fraud Charter’ *Which?* (18 December 2024) <www.which.co.uk/policy-and-insight/article/a-year-on-from-the-online-fraud-charter-aeFBu4h2Pre8> accessed 2 July 2025.

¹²²Department of Culture, Media and Sport, *Online Advertising Taskforce - progress report 2023–24* (2 December 2024) <www.gov.uk/government/publications/online-advertising-taskforce-progress-report-2023-24> accessed 2 July 2025.

¹²³ASA system submission to the Department for Digital, Culture, Media and Sport’s Online Advertising Programme consultation (8 June 2022) 2, 8–10 <www.asa.org.uk/static/ab956c83-5797-4158-81695c67632304c9/OAP-ASA-System-FINAL-Response-8-June-2022.pdf> accessed 10 July 2022.

¹²⁴See e.g., Michael Veale and Frederik Zuiderveen Borgesius, ‘Adtech and Real-Time Bidding under European Data Protection Law’ (2022) 23(3) *German Law Journal* 226 for an analysis of structural/legal issues in ad-delivery systems and infrastructure-level risks.

¹²⁵Department of Culture, Media and Sport, Statement UIN HCWS272 (n 17).

Recent Parliamentary interest underscores the ongoing regulatory uncertainty but there appears little momentum for legislative intervention. In June 2025, Conservative MP Damian Hinds asked whether the government would take steps to regulate programmatic advertising, a key vector for fraud, but received only a holding reply. The Minister, Chris Bryant, confirmed that the government would ‘continue to monitor the regulatory framework’,¹²⁶ while relying on the taskforce to pursue non-legislative measures on addressing illegal advertising. This exchange signals a procedurally engaged but substantively cautious OAP orientation, arguably reflecting at present some reluctance to commit to structural reform.

Conclusions

While the OSA introduces important duties for platforms to prevent, minimise, and remove fraudulent ads, several unresolved issues might limit its effectiveness. Although the services’ advertising-based business model is seen by some as contributing to the content problems on those services, and potentially provides a route for money-laundering and fraud, the Act was never a comprehensive advertising statute. Its Part 3, Chapter 5 narrowly targets fraudulent ads, while unchanged core definitions leave uncertainty about the reach of the general illegal content duties into paid-for advertising. More specifically, our reading of the OSA’s relevant provisions has identified a number of potential concerns.

First, the distinction between fraudulent ads and ad fraud is conceptually underdeveloped in the legislation, with the latter largely escaping the scope of the Part 3, Chapter 5 duties. The result is a patchwork: strong on fraudulent-ad content within walled gardens; thin on systemic placement risks. Moreover, that Chapter imposes different obligations in relation to fraudulent ads on U2U services from search services. The content to which these Chapter 5 duties about fraudulent ads apply is narrower than the content covered by the duties in the other parts of the Act that apply to U2U and search services. This leaves a potential gap in protections and enforcement relating to advertising.

Second, *small* U2U and search services are not covered by the Chapter 5 duties. This also leads to significant gaps in fraudulent ad protections, including for children. Although the statutory instruments underpinning the categorisation rules are now in force, ‘small but risky’ platforms remain excluded, limiting fraudulent ads provisions to large Category 1 or Category 2a services, even though these have not yet been named. The High Court’s dismissal of the Wikimedia challenge removes uncertainty about the validity of the Categorisation Regulations, but scope remains unsettled until Ofcom designates services

¹²⁶Question for the Department for Culture, Media and Sport, UIN 61137, tabled on 19 June 2025 and answered on 30 June 2025 <<https://questions-statements.parliament.uk/written-questions/detail/2025-06-19/61137>> accessed 8 July 2025.

under those Regulations. Any remaining litigation risk is designation-specific, not regulation-wide. The inconsistency in how duties apply to user-generated content vs paid-for advertising further complicates enforcement, particularly with ambiguities around the definition of ‘users’ and how this affects advertisers. A further asymmetry is the coexistence of a statutory safety regime with a privately coordinated anti-fraud track (e.g. Meta’s FIRE under ‘Regulation of ad content’ earlier), the latter governed mainly by data protection law and sectoral controls rather than Ofcom’s remit (useful in practice, but an odd two-lane system that splits accountability with no single regulator clearly in charge).

Third, definitions in the Act itself are unclear: a ‘user’ (for the purposes of ‘user-generated content’) could include advertisers uploading content to a service as well as individual users generating their own text or image-based content; the ‘service’ (for the purposes of sharing the content that is regulated by the Act) could include the advertising delivery service as well as the user interface. Importantly, different interpretations of these terms have significant implications for the scope of the duties: under the most expansive interpretation of ‘user’ and ‘service’, all advertising linked to Schedules 5–7 of the OSA comes into scope of the illegal content duties but only for U2U services *as well as* the content listed in s 40 (‘fraud etc. offences’) coming into the scope of specific fraudulent ad duties for U2U and search services. Also, under the most expansive interpretation, obligations would apply to advertising content on U2U as the general rules are already in force or shortly to be in force in respect of content harmful to children (from 25 July 2025).¹²⁷ These alternatives are mapped in Table 1 and inform the Readings A/ B discussion earlier.

In short, what we term as Reading A appears to be the baseline for compliance now; it tracks the search carve-out under the Act and Ofcom materials, preserving policy intent, but it leaves illegal, non-s 40 paid ads on U2U outside the general duties. Reading B is textually credible and widens U2U exposure to illegal-content duties (Table 1 summarises possible outcomes and flags the contested limb, i.e. advertisers-as-users). Reading B gives full effect to ss 55(3) and 227 read together and avoids an odd split between organic and paid content on the same interface, but it arguably strains the policy-aligned reading and surfaces an asymmetry with the explicit search carve-out. Pending Ofcom’s fraudulent-ads Code, we recommend adopting Reading B in Ofcom’s General Part 3 illegal content guidance for U2U services (treat advertisers as ‘users’ for s 55(3) when their material is supplied to the same consumer-facing interface as end-users),¹²⁸ with a

¹²⁷Ofcom, ‘New Rules for a Safer Generation of Children Online’ (24 April 2025) <www.ofcom.org.uk/online-safety/protecting-children/new-rules-for-a-safer-generation-of-children-online> accessed 4 July 2025.

¹²⁸We include the ‘same consumer-facing interface’ limiter to keep Part 3 focused where the Act puts it: on a U2U service and the people who use that service. Treating the open programmatic stack as ‘users’ would extend ss 55(3) and 227 beyond their ordinary meaning, potentially blurring duties owed by the platform with activities of separate advertising infrastructure.

cross-reference in the Chapter 5 Code; and retaining the search exemption so the U2U/ search split remains text-faithful. This is administrative interpretation (not re-legislation) clarifying application within the existing scheme; adjudication of meaning ultimately rests with the courts.

Fourth, paid-for adverts are included in the general U2U provisions but are not included in the general search provisions. The exclusion of paid-for ads under the general Part 3 duties for search services while seemingly including them for U2U services creates a potential loophole that undermines consistency and potentially weakens enforcement coherence. Notably, a wider interpretation of these general duties for U2U platforms could relieve some enforcement pressure from the ASA, which currently lacks formal leverage under the OSA (it might enable the ASA to act as a trusted flagger or take on a more integrated enforcement role). This advantage, however, would not extend to search services, underscoring a further limitation of the current regime. This disparity suggests that platforms like social media may face stricter oversight than search engines, despite the similarity in the risks posed by illegal ads across both types of service. As noted, however, Ofcom's published materials do not treat paid-for ads as user-generated content and so they are exempt from the general Part 3 rules,¹²⁹ which are now in effect and enforceable as of 17 March 2025.¹³⁰ While this interpretation may be a practical approach to the issue, it also means that stronger user protections – which would have now taken effect had a broader reading been adopted – have not materialised.

Finally, the regime does not directly duplicate the ASA obligations but complements them by placing responsibility on platforms. However, it still leaves search services outside the scope of this potential benefit, and leaves room for external advertising delivery systems to escape oversight¹³¹ – a significant gap that OAP initially appeared poised to address but does not. As noted, while 'walled garden' environments are potentially caught by OSA, the open ads market remains outside the OSA regime. This regulatory asymmetry reflects a deeper structural issue also identified by the Commons Select Committee on Social Media, which concluded that the government's reliance on industry-led, content-focused interventions fails to address the monetisation of harmful content through advertising and expressed scepticism that the industry can or will effectively self-regulate.¹³² The Committee's observations underline the concern that current approaches remain too

¹²⁹See the discussion under 'Identifying the boundary between the general rules and Chapter 5 rules' as well as Ofcom, *Protecting children from harms online – Vol 2* (n 113) 44 and Ofcom, *Protecting people from illegal harms online – Annex 1* (n 112) 68 (scope query on programmatic advertising and Ofcom's response).

¹³⁰Ofcom, 'Quick guide to illegal content codes of practice' (n 119).

¹³¹This article has not discussed the impact of data protection rules on the open display market, but it is submitted that those rules would not deal with all the issues in any event. See also (n 6).

¹³²SIT Committee, *Social Media, Misinformation and Harmful Algorithms* (n 3) para 97.

content-centric and deferential to industry self-governance. Overall, while the OSA framework strengthens platform responsibilities, its relatively narrow scope, the uncertainty of its application across different services, and unaddressed external ad delivery processes leave some vulnerabilities in place.

Acknowledgment

Some of the foundational analysis in this article was first outlined in a shorter piece published on 13 June 2025 on the Online Safety Act Network webpages: <www.onlinesafetyact.net/analysis/advertising-and-the-online-safety-act/> accessed 28 June 2025. The present contribution substantially extends, systematises, and deepens that earlier work.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Lorna Woods, OBE is Professor Emerita at the University of Essex. Formerly a Professor of Internet Law and a member of the Human Rights Centre, she has worked in the field of media and communications regulation for more than thirty years, publishing on both domestic and European law. From 2018 to 2023, she worked with Carnegie UK Trust on a project on the reduction of harm in social media and is now a consultant to the Online Safety Act network. She is an Affiliate Fellow at the Minderoo Centre for Technology and Democracy at Cambridge University as well as a member of the policy network at the Centre for Science and Policy there.

Alexandros Antoniou is a Senior Lecturer in Media Law. He researches influencer marketing, online safety, and intellectual property asset management. His work in these areas has been published in leading journals such as *The Journal of Media Law*, *Communications Law*, *Entertainment Law Review* and *the Journal of Intellectual Property Law and Practice*. He is a Senior Fellow of the Higher Education Academy and a legal correspondent for the Council of Europe's European Audiovisual Observatory, contributing comparative legal intelligence for regulators and rights-holders across 40+ countries.

ORCID

Alexandros Antoniou  <http://orcid.org/0000-0002-4249-0939>