Behavioural Audit of Online Services with Advertisement Functionalities:

Methodology Paper

Report

Published 10 July 2026

Contents

Overview

This report outlines the methodology used by Ofcom's Behavioural Insight Hub to examine advertising functions on major online platforms. The research supports the development of regulatory codes of practice under the UK Online Safety Act (OSA), specifically focusing on duties relating to fraudulent advertising. Using researcher-created accounts with structured, screen-recorded journeys across several platforms, the study systematically maps platform design features, sign-up processes, advertising workflows, reporting mechanisms, and account security features. The methodology is carefully designed to replicate snapshots of real-world user experiences while maintaining stringent data protection and safeguarding standards.

The audit provides evidence to inform Ofcom's regulatory approach, identifying how platform design within advertising functionalities influences user (including advertiser) behaviour, existence and persistence of fraudulent advertisement and online safety. The study does not assess individual users or advertisers but rather documents and analyses the systems and processes shaping online advertising ecosystems. The research employs a similar methodology as the previous behavioural audit.[1] The findings from this audit are presented separately in an accompanying slide pack, which synthesises the key cross platform observations identified through the audit. Key findings include a systematic comparison across platforms and how platform design features, and Online Choice Architecture (OCA), could potentially influence user/advertiser behaviour and online safety.[2]

Behavioural Audits – In Summary

- Behavioural audit methodology allows for structured observation of platform interfaces and user journeys, identifying how design features may influence behaviour, including potential risks for fraudulent advertising.
- Researcher accounts, including an adult user, an ad manager, a business account, and a non-logged in access, replicate typical user pathways without using real personal identifiers.
- Screen recording and secure data storage enable detailed analysis of platform design, prompts, and reporting mechanisms, through a comprehensive taxonomy and structured codebooks.
- Four areas of interest were investigated: sign-up and checks, ad creation workflows, reporting mechanisms, and account takeover/security features.
- Ethical and safeguarding protocols include engagement rules, partial redaction of identifiers, and a comprehensive Data Protection Impact Assessment.
- Limitations include differences in platform algorithm responses and the inability to measure prevalence of fraudulent advertising.

[1] Ofcom, 2025, A behavioural audit of online services in the UK (technical report).

[2] Online choice architecture (OCA) refers to the design of digital environments that influences how individuals make decisions and interact with online platforms. Based on the Competition and Markets Authority (CMA) definition, this comprises three components: Choice structure: how options are designed and presented, Choice information: how users receive information about their choices, and Choice pressure: indirect influences affecting decisions. OCA impacts user behaviour through design elements such as option order, default settings, and the complexity of accessing controls. It also includes how information is presented (e.g., clear vs. dense terms of service) and features that apply pressure, like time-limited offers. Competition & Markets Authority. (2022), Online Choice Architecture: How digital design can harm competition and consumers.

1. Introduction and Research Aims

Online platforms are central to the distribution of paid-for advertising, including content that may constitute fraud or financial crime. The UK's Online Safety Act requires certain online service providers to implement proportionate systems and processes to mitigate risks associated with fraudulent advertising. This research aims to provide evidence for effective regulatory measures by auditing how advertising systems function in practice and identifying vulnerabilities within user/advertiser journeys.

The behavioural audit does not assess individual users or advertisers but systematically documents platform design features and processes influencing the creation, dissemination, and reporting of advertisements. The objective is to inform regulatory codes by highlighting points in platforms' designs and features where fraudulent advertising may arise or persist.

2. Overall Research Design

2.1 Behavioural Audit Approach

The study utilises a behavioural audit methodology, involving structured observation of platform interfaces and user journeys with accounts created specifically for research purposes. This approach avoids reliance on self-reported data, directly examining how platform design and choice architecture influence user/advertiser behaviour and risk exposure. Direct observation allows systematic comparison across platforms using a common analytical framework.

2.2 Platforms Covered

- YouTube
- TikTok
- Google Search
- Facebook
- Instagram
- Microsoft Bing (Search)
- Reddit

Platforms were selected based on their relevance to paid-for advertising and inclusion within the scope of the Online Safety Act. For each platform, we also selected certain parts of the service (referred as "feeds") to be included in the audit.[3]

Feeds selected for the audit

Table 1: Feeds selected for audit across the platforms

Platform	Feeds selected
Facebook	Facebook Home, Facebook Reels
Instagram	Instagram Personal Feed, Instagram Reels, Instagram Search and Explore page
Google	Google Search, Google Shopping

[3] The audit examined features and functionality available during the ad creation and reporting processes within these feeds. Content appeared in these feeds were not in scope of this research.

YouTube	YouTube Home, YouTube Search, YouTube Shorts
Reddit	Reddit Homepage, Reddit Search
Bing	Bing Search
TikTok	TikTok Explore, TikTok For you

The platforms were notified that the audit was being conducted, and a transparency notice was published on the Ofcom website to inform the public about the research.[4]

3. Researcher Accounts

Data collection was conducted between October and November 2025 using researcher created accounts operated by trained Ofcom researchers. Four access types were used: adult personal accounts (18+), business accounts (where differentiated), ad manager accounts (where offered) and non-logged in browsing. Fictional names, randomly generated dates of birth, gender identifiers (only where required), and unique, non-Ofcom email addresses were used to ensure functional access without using personally identifiable information.

Research was conducted on Ofcom-owned devices, used exclusively for this project and operated within Ofcom offices. Devices were securely stored when not in use, and fieldwork followed a structured schedule.

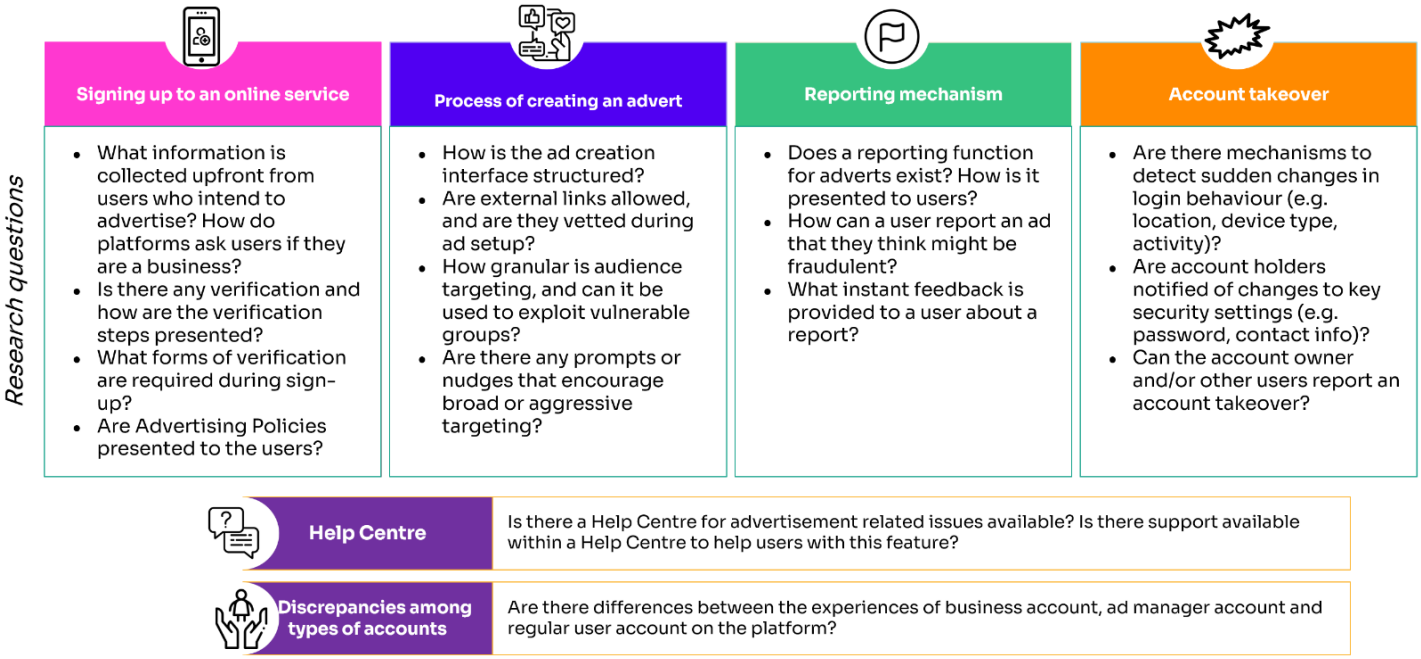
4. Key areas and User Journeys

4.1 Key Areas

- Sign-up and check processes: Examining identity checks, advertiser checks, and friction points at account creation.
- Advertisement creation workflows: Mapping the steps to create an advertisement, including prompts, defaults, review stages, and safeguards.
- Reporting mechanisms: Assessing user ability to report advertisements, clarity of reporting pathways, and required effort.
- Account takeovers and security features: Observing platform features to prevent or respond to unauthorised account access.

[4] Transparency notice: Research on online platforms to explore online safety

Figure 1: Key areas and research questions



4.2. User Journeys

We outline all of the journeys completed as part of the audit, with supporting explanations given below.

Table 2: Journey completion across key areas

	Sign-up process	Creating an Ad	Reporting Mechanism	Account Takeover
User Account	Complete	Complete	Complete	Complete
Business Account	Complete	Complete	Complete	Complete
Ad Manager	Complete on browser-version only	Complete on browser-version only	Complete on browser-version only	Complete on browser-version only
Non-logged User	Non-complete due to platform's rules	Non-complete due to platform's rules	Complete	Non-complete due to platform's rules

4.3 Researcher Behaviour and Rules of Engagement

Researchers followed a strict non-interaction protocol, avoiding engagement with content or users. Accidental interactions were recorded and assessed as minimal impact. Researcher accounts

followed the ad creation process without submitting ads. To investigate the reporting functionality, one benign ad was reported when available.

5. Data Collection

5.1 Developing a framework and a codebook for the audit

To underpin the audit, a rapid evidence review was undertaken, focusing on the online choice architecture (OCA) of the platforms within the four identified areas of interest. This review drew upon research from Ofcom, the Competition and Markets Authority (CMA), and other emerging studies in the developing field of OCA practices on social media.[5] In addition, Ofcom's A-Sparc model was considered, contributing to the development of a taxonomy categorising OCA practices observed during the audit.[6] The list of relevant OCA practices can be found in the table below.

Table 3: Relevant OCA practices

Choice structure			
• Defaults • Ranking • Partitioned pricing • Bundling • Choice overload and decoys	• Sludge • Dark nudge • Trick wording • Visual interference	• Irreversibility • Cooling off period • Click-wrap agreements • Comprehensive acceptance	• Sensory manipulation • Forced action/outcomes • Hidden options • Tiered responses • Nagging • Asymmetric options • Disguised ads
Choice information			
• Drip pricing • Framing • Prompts to reconsider • Sneaking	• Comparison prevention • Tool transparency • Limited feedback • Private feedback	• Intervention prompts • Overwhelming options • Lengthy text • Complex text	• Ambiguous language • Unclear repercussions • Positively framed restrictions • Ad labelling
Choice pressure			
• Commitment • Prompts and reminders	• Notifications • Fake scarcity • Fake social proof	• Social accountability • Social proof cues	• Countdown timers • Fake urgency • Personalisation • Subscription traps

[5] CMA, 2022 and Ofcom, 2025.
[6] Ofcom, 2021, The A-SPARC model of online platforms.

The resulting taxonomy distinguishes between 'dark', 'grey', and 'bright' patterns. Dark patterns refer to deliberate design strategies that may mislead or pressure users into actions that are not in their best interests. Grey patterns are more ambiguous, with their effects varying according to user preferences and context at times nudging users in ways that may not align with their interests, while in other instances enhancing their experience. Bright patterns, by contrast, are practices that promote trust, loyalty, and respect, supporting users in making informed and intentional choices without undue influence, and thereby fostering a more balanced and user-centric experience.

Developing the codebooks

This taxonomy was integral to structuring the codebook used for data collection, with the codebook containing detailed questions tailored to each key area. Researchers systematically responded to these questions throughout the audit process.

To support consistency in coding and uphold a rigorous methodological approach, the codebook included detailed annotations. Multiple workshops and weekly meetings were held, enabling researchers to cross-check coding decisions and align their interpretations of instructions and definitions. While the qualitative nature of the research meant some degree of individual interpretation was inevitable, uncertainties were routinely addressed through collaborative discussion. This ensured a coherent and uniform approach to coding across all data collection activities.

5.2 Screen Recording and Capture

Screen recording was the primary data collection method, capturing complete user journeys. Recordings included interface layouts, prompts, default settings, decision points, and content that appeared on relevant feeds.

5.4 Ethical, Safeguarding, and Data Protection Considerations

Research was conducted under a comprehensive Data Protection Impact Assessment, with safeguards including minimisation of data collection, avoidance of active user engagement, partial redaction of identifiers, strict access controls, and procedures for handling illegal or harmful content. A safeguarding guidance document was developed for the audit and applied throughout the fieldwork. This guidance sets out the procedures to be followed if researchers are exposed to potentially illegal or harmful content. It also provides broader safeguarding and wellbeing guidance for researchers and has been developed in line with Ofcom's wider Colleague Safeguarding Policy. Transparency was maintained through service engagement and publication of an updated transparency notice. (Transparency notice: Research on online platforms to explore online safety)

6. Data Analysis and Reporting

The analysis phase focused on identifying platform design patterns, assessing consistency and variation across services, and pinpointing potential risk areas relevant to fraudulent advertising. Researchers used a structured codebook, with senior researchers quality-assuring at least 10% of user journeys. Findings were synthesised from coded data and collaborative discussions, and were reported transparently. Reporting of the findings gave prominence to platform design features, cross-service differences, and regulatory risk points, all contextualised within the specific timeframe

of the audit to reflect the dynamic nature of online platforms.[7] The outputs from this analysis are available here.

7. Limitations

There are three key limitations to note regarding the audit methodology and findings. First, the use of researcher accounts may not fully reflect the experiences of long-standing or typical users, as platform algorithms could interact differently with these accounts. Second, the audit presents only a snapshot of platform features and functionalities as they existed during October and November 2025; platforms frequently update their services or cached content, so some details described may no longer be current. Importantly, this audit did not aim to measure the prevalence of fraudulent advertising but instead focused on examining system design and operational processes during the period of study. A further limitation is that the methodology did not involve publishing adverts or running advertising campaigns over time. This was a deliberate design choice, grounded in ethical and safeguarding considerations. As a result, researcher accounts may not have triggered certain automated checks, escalations, or bespoke checks processes that could be activated following sustained advertising activity, higher spend, or exposure to a wider range of products or services.

[7] We do not identify any platform in any of the published findings. All findings are anonymous, and where necessary platform names are redacted.