MRS Awards 2024 Winner Business Impact of the Year - UK

MRS Awards 2022 Finalist Business-to-Business Research

MRS Awards 2020 Winner Innovation of the Year

MRS Awards 2019 Winner Global Agency of the Year

MRS Inclusion Pledge

STRAT 7 JIGSAW | Ofcom

Online Safety Business Survey

Research Summary

September 2026

MAKING SENSE OF HUMAN COMPLEXITY

Contents

1 Foreword

As the UK's independent regulator for online safety, Ofcom's role is to implement and enforce duties set out in the Online Safety Act ('the Act'). Since the Act received Royal Assent in October 2023, duties related to illegal content, protecting children from harmful content, implementing age assurance, and governance processes have come into effect on a phased basis.

The OSA covers a very wide range of services, with more than 100,000 sites and apps in its scope ranging from micro businesses to some of the biggest tech companies in the world. We have built particularly close supervisory relationships with services that we expect to pose particular risks to users, both large and small. But we have also worked to make online safety regulation as easy as possible to understand and achieve for all service providers, and have provided a number of tools and resources to promote compliance, particularly aimed at small firms.[1] This research is intended to help us understand perspectives amongst this wider universe of services, to support the development of these tools, target our communications to industry more effectively, give us insight into possible barriers to compliance, and test whether services have sufficient and accurate understanding of the Act's requirements. This enables us to prioritise our engagement and helps us target our efforts to raise awareness and drive compliance as effectively as possible.

In order to explore how regulated services are responding to the Act, Ofcom commissioned a quantitative survey among employees responsible for online safety in 125 micro, small, medium, and large online services that support user-to-user interactions, allow users to access, post, or share pornographic content, or function as search engines. The survey was supplemented by a small number of qualitative interviews.

While it is impossible, given this diversity, to target a fully representative sample of in-scope services, we set minimum quotas in order to ensure that the sample reached a variety of platforms, spanning different business sizes, service types, and regions, including the UK, the rest of Europe, and the US. No weighting was applied. Responses rely on individual respondents' knowledge and perceptions, which may be limited in some instances and may not fully reflect the views or practices of their organisation. As a result, the findings provide insight into the experiences and perspectives of a diverse range of services but should not be interpreted as statistically representative of the wider population of online services in scope of the Act.

The findings of the research cover services' awareness and attitudes towards the Act, implementation of required duties and the costs and barriers associated with compliance, as well as the systems and processes they currently have in place. The results show that awareness of the Act is high and attitudes towards the Act are mixed. Over half of services surveyed claim to have 'fully' or 'mostly' implemented the Act's requirements. The most common actions taken by services were introducing age assurance and strengthening content moderation, alongside conducting risk assessments. Still, some services recognise that they still have a way to go to comply with the safety duties in the Act. Financial constraints and resource limitations were the most frequently cited barriers to compliance. The organisations that have made changes to their service, and borne more substantial costs than others, tended to be those that allowed pornographic content or had experienced their users being exposed to illegal content or child users experiencing harm.

The duties that service providers need to comply with are subject to factors specific to each individual service, such as the service type, its user base, and the functionalities it has available. While this research provides a snapshot of services' experiences reading and responding to the Act, it was not designed to assess compliance with the Act's requirements: i.e. it is not possible to know which specific measures the surveyed services should be deploying, and so levels of compliance with measures such as highly effective age assurance cannot be determined.

[1] See also: ofcom.org.uk/online-safety/illegal-and-harmful-content/guide-for-services

2 Background and objectives

2.1 Background

The Online Safety Act received Royal Assent in October 2023. It applies to a diverse range of services that host user-generated content (like images, videos and comments) or which allow UK users to interact with each other online through messaging, forums and comments, search services, and services that display pornographic content. The Act places a range of duties on regulated services including in relation to illegal content and content harmful to children.

Ofcom is the regulator for online safety in the UK, under the Act. Its job is to make sure regulated online services, like websites and apps, meet their duties to protect their users. Ofcom undertakes numerous tasks, such as publishing Codes of Practice with safety measures that certain services are recommended to implement, and driving companies' compliance with the Act.

For example, the Act places duties on certain regulated services to implement highly effective age assurance. This includes the use of highly effective age assurance on user-to-user services likely to be accessed by children to ensure that minors of any age are prevented from accessing pornography, suicide, self-harm, and eating disorder content and to ensure that they are not normally able to encounter pornography on online adult sites.[2] In addition, Ofcom's Protection of Children Code of Practice for user-to-user services (Protection of Children Code) recommends that certain regulated service providers use highly effective age assurance to protect children from other forms of harmful content, including (but not limited to) content which is abusive, hateful, and violent.[3] Ofcom has published guidance to assist regulated service providers in understanding whether an age assurance process is highly effective and complying with their duties under the Act.[4]

To be as effective as possible at implementing the Act and driving compliance to keep people safe online, Ofcom needed to understand services' awareness and attitudes towards the Act, levels of implementation, safety measures currently in place, barriers to compliance, and the impact of the Act on services.

2.2 Research objectives

Specifically, the research needed to provide the services' views on the following questions:

- To what extent are services **aware** of the Online Safety Act and what are their attitudes towards it?
- To what extent have services **implemented** measures to improve online safety?
- What online safety systems and processes do services **currently have in place**?
- What **barriers** have prevented services from complying with the Act and what has been the **impact of implementation** on services?

[2] Section 12(4)-(6) and section 81(2) of the Act.
[3] Further details on the duties relating to the protection of children in the Act can be found in the Legal framework in our April 2025 Statement: Protecting children from harms online (our April 2025 Statement).
[4] See ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance

3 Research methods

A total of 125 quantitative interviews and 10 qualitative interviews were completed by STRAT7 Jigsaw, on behalf of Ofcom, between 2 February and 3 April 2026.

3.1 Sample and recruitment

As our target audience of employees of regulated online services with responsibility for online safety was highly specific, we utilised a multi-path recruitment strategy. This involved matching apps or websites with employees and reaching out to them individually on LinkedIn. We began by compiling a long list of relevant apps or websites based on the type of service and other relevant factors. These services were then matched to company names using LinkedIn, and we validated the service categorisation by reviewing each company's LinkedIn description, adding any details required for our quotas. Using LinkedIn personal profile data, we then built a preliminary candidate database and appended additional contact information. We then identified job titles potentially in scope for this research, taking into account service type and company size, and refined the long list of individuals to a shorter list where both the company and the employee appeared suitable.

Verified candidates were then contacted with information about the research, including confidentiality assurances and incentive details. Finally, we confirmed their contact information, assigned each person with a unique, trackable, password-protected survey URL, and invited them to complete the survey.

Once in the survey, potential participants were screened further to check they were the right individual for the interview. All participants had to be responsible for online safety[5] on a platform that supported user-to-user interactions and/or allowed users to access/post/share pornographic content and/or functioned as a search engine. In addition, the platform was required to have a significant number of UK users or have the UK as a target market.

3.2 Quantitative survey

3.2.1 Fieldwork

The survey design was tested in a series of **enhanced cognitive pilots** (10 interviews) to check and optimise comprehensibility, mitigate misinterpretation and avoid any ambiguity, after which the questionnaire was refined. A further sub-sample of 25 quantitative interviews was conducted as a **mini-pilot** to validate the survey design and recruitment approach. This was followed by the **main fieldwork rollout**, which included an additional 100 interviews. Throughout each phase, recruitment quotas and participant responses were closely monitored.

3.2.2 The questionnaire

The questionnaire began with a series of screening questions. To ensure a good representation of different 'in-scope' services among the 125 quantitative interviews, minimum quotas were set on the following criteria:

- Headquarters location: UK > 30, Europe > 30, North America > 30

[5] Note: The screening question was worded as follows: "Do you have responsibility for any of the following areas (either solely, jointly, or as part of a team)?". To proceed to the next screening question, respondents were required to select "Online safety" from the list of options.

- Number of employees: Micro (1-9) > 25, Small (10-49) > 25, Medium (50-249) > 25, Large (250+) > 25
- A minimum of 5 in various types of online platform (e.g. discussion forums, social media, gaming, dating, pornography, and others)

For analysis purposes services were categorised as either a 'pornography or reported risk' service (48% of the total sample) or 'Not operating a pornography or reported risk' service (52% of the total sample). The definitions are below alongside the proportion of the respective sample they account for:

- **'Pornography or reported risk' service**: 48% of the total sample - defined as having one or more of these four characteristics:

The platform was a pornography site	*32% of pornography or reported risk respondents*
Users were able to post/share pornographic content	*25% of pornography or reported risk respondents*
Any users had encountered illegal content/behaviour	*67% of pornography or reported risk respondents*
Any child user had encountered content that is harmful to children	*17% of pornography or reported risk respondents*

- **'Not operating pornography or reported risk' service**: 52% of the total sample - defined as any platform not classified as a 'pornography or reported risk' service

The main survey then explored awareness, understanding, and attitudes towards the Act, including whether organisations consider themselves in scope, actions taken or planned in response, barriers to implementation, perceived costs, and overall sentiment. Subsequent sections examined governance practices, awareness of illegal or harmful content being available on their platforms, and content moderation and user reporting systems.

3.2.3 Data integrity

Given the thoroughness of the recruitment approach, the probability of fraud was extremely low, however, we implemented the following measures to prevent fraud and low-quality data on our quantitative surveys:

- Checked IP addresses to ensure no duplicate respondents
- Captured job title and checked back to LinkedIn profile
- Checked for flatlining (providing identical response to a series of questions without considering the differences in the statements) and speeding (answering questions too quickly to have reasonably given sufficient thought to the response)
- Checked for inconsistent answers
- Sense checked all verbatim responses and followed up with anything that needed clarifying

3.3 Qualitative interviews

A total of 10 qualitative interviews were also conducted. Each interview lasted between 45 and 60 minutes and took place via video call. The same recruitment methodology was used, with minimum quotas set on service type, headquarter location, and business size to ensure that a diverse mix of services were represented.

The discussion guide broadly mirrored the questionnaire's structure, covering profiling, awareness and attitudes to the Act, and organisational responses, including implementation, challenges, costs, and future plans. However, it was exploratory in nature, focusing on depth and context by probing on decision-making, perceived impacts, reactions, and implementation journeys.

3.4 Caveats on interpreting the results

When reading this document, please note the following:

- The aim was to hear from a range of voices and recruit a good spread of service types, rather than to achieve a sample that is fully representative of regulated services. Considering that the sample has not been weighted to be representative of the target universe and the relatively small sample size, the results should be interpreted with caution, particularly when examining or comparing specific sub-groups. In light of this, results have not been tested for statistical significance.
- Individual employee responses may not necessarily reflect the position of the organisations they work for. Responses rely on employees' perceptions and knowledge of their organisations' practices, which might in certain instances be more limited, or might require them to rely on estimates, particularly when it comes to areas not directly involved in their day-to-day role. In the results section of the report, the term "services" is sometimes used to refer to responses provided by employees of service providers.
- As with any research, some chose not to take part. Non-response may arise from a range of factors, including a lack of interest in the topic or limited availability. Despite taking steps to reassure respondents about confidentiality, there remains a residual risk of self-selection bias, whereby organisations that perceive themselves to be less aligned to the Act may be less likely to take part. Similarly, some behaviours or experiences, particularly sensitive or potentially non-compliant ones, may be under-reported.
- The question of whether a specific code measure applies will depend on the size of the service, the level of risk, and whether it meets other specific criteria, which this survey does not determine in detail and so levels of compliance with specific measures cannot be determined.
- This project represents a snapshot in time from February to April 2026.

4 Summary of findings

This section summarises the key findings of the research. For more detailed results, readers should refer to the questionnaire and data tables published alongside this report.

4.1 Awareness of and attitudes towards the Online Safety Act

Awareness of the Act was generally high among the regulated services we heard from,[6] with one in three reporting in-depth familiarity. Overall, attitudes towards the Act were mixed. Many, particularly the larger businesses (250+ employees), were broadly positive, with a clear emphasis on the importance of protecting users, especially children. However, a sizeable minority, driven largely by those providing 'pornography or reported risk' services,[7] were more sceptical, questioning its effectiveness. Concerns mainly related to cost, complexity and the clarity of requirements.

- **The majority of respondents were aware of the Act.** Most (87%) claimed to have heard of the Act before their interview. However, awareness was not universal, with over one in eight lacking any clear recollection of the Act (8% reported no knowledge and 5% were unsure).
- **However, fewer respondents had in-depth knowledge of the Act or had spent a lot of time thinking about it and how it applies to their organisation.** Among those aware of the Act, four in five (80%) said they knew at least a fair amount about it, including two in five (41%) who said they knew "a lot" or "quite a lot". However, respondents were somewhat less likely to have considered what the Act means for their own organisation: while just over half (52%) said they had given this "a lot" or "quite a lot" of thought, almost a quarter (23%) had given it only "a little" or "not a lot" of thought.
- **Most participants believed their platform was within the scope of the Act.** Four in five (80%) recognised that their organisation provided a regulated service, while around one in ten (9%) thought it did not apply to their organisation, and a further one in ten (11%) were unsure.
- **Around half (47%) felt favourably towards the Act.** Attitudes were particularly positive for large businesses (250+ employees) and those not operating 'pornography or reported risk' services. Participants were most likely to agree that the Act will 'help to keep children safer online' and 'establish more consistent standards', with three in five (61% and 60% respectively) agreeing with each statement.
  - This was reinforced by the qualitative findings, which showed broad agreement that protecting children was a key priority. Additionally, the qualitative research emphasised the importance of businesses recognising and buying into the underlying purpose of the Act. It was seen as helping to raise awareness of user risks, and there was a broad sense that protecting people is the right course of action. The Act was also viewed by many as providing useful guidance and a clear rationale for addressing harmful behaviour. Some qualitative participants described it as the 'gold standard' leading on safety standards, with other countries likely to follow suit.
- **However, approximately one in three (35%) services held unfavourable views of the Act.** This was largely driven by those operating 'pornography or reported risk' services, those headquartered in North America, and micro businesses (1-9 employees). Just over half of respondents agreed that the Act was 'expensive to implement' (58%) and nearly half (46%) agreed that 'the requirements were difficult to understand'.

[6] Note: whenever this report attributes responses to *services*, it is referring to responses provided by an employee of a service.
[7] See definition above at 3.2.2.

- The qualitative interviews revealed several concerns, particularly around guidance that was viewed as unclear, overly burdensome, or excessively long and technical. Some participants also pointed to ambiguity in the Act's scope, noting that it seemed primarily designed for social media platforms and did not always align neatly with their own operations. In addition, certain elements were described as open to interpretation, contributing to uncertainty about the specific actions required. Others spoke about the challenges and costs associated with the implementation of the Act – for example, one service was paused, as the service stated they couldn't easily implement age assurance at that time for technical and resource reasons. This was a porn site with an international customer base, so they temporarily shut down the UK site while they prepared necessary changes to it. Another had to transfer their user forum to Facebook, as they felt they couldn't afford or resource the additional moderation requirements.

4.2 Reported actions taken by service providers due to the Online Safety Act

Almost half of the participants said that their organisation had made changes in response to the Act, while three in five said they have 'fully' or 'mostly' implemented the required safety measures. The most common actions included introducing age assurance and strengthening content moderation, alongside conducting risk assessments. Services recognised that compliance involves a mix of quick wins and more complex, resource-intensive changes. The qualitative research established that drivers of action ranged from legal obligations and reputational risk mitigation to a commitment to user protection.

- **Three in five (59%) said they mostly or fully implemented the Act's requirements.** This includes services who believe that their pre-existing systems and processes were already largely compliant with the Act and those who made changes to ensure that they are mostly or fully compliant.
- **Two in five (44%) of all services surveyed said they have implemented changes in response to the Act.** Among those aware of the Act, half (50%) reported making changes, while a quarter (25%) had not yet done so, and another quarter (25%) believed no changes were needed.[8]
- **'Pornography or reported risk' services were more likely to say they had made changes in response to the Act (53%).**
- **The most common actions taken in response to the Act were the implementation of age assurance and the strengthening of content moderation practices**. Around half (51%) of those that had made changes had introduced age assurance methods,[9] while two in five (40%) had enhanced content moderation.

  - The qualitative research indicated that services had a range of responses to the introduction of the Act. Some businesses embraced the Act as a positive driver, using it to strengthen their approach and enhance their reputation or competitive positioning – particularly where trust and safety were already core to their brand. Others responded more defensively, focusing primarily on mitigating perceived risks from sanctions and reputational damage.

[8] This research was not designed to ascertain compliance levels. The results reflect respondents' perceptions regarding their organisations' compliance and actions taken in response to the Act. The research also did not seek to establish whether services were already compliant with the Act before it came into force, therefore not having made changes in response to the Act may not necessarily imply that services are not compliant, i.e. it could also mean that services did not take the time to consider the Act yet.
[9] This includes a range of age assurance methods, some of which may meet the requirements of being highly effective.

- **Among those yet to implement any changes in response to the Act, the most common plan for the future was to introduce age assurance.**[10,11] Services also planned content moderation improvements, while some were unsure what steps to take.

4.3 Systems and processes currently in place

The Act requires in-scope services to conduct risk assessments for illegal content and children's access assessments, to establish whether their service is likely to be accessed by children. Where a service is likely to be accessed by children, it needs to conduct a risk assessment for content harmful to children.

At the time the survey was undertaken, two in three reported having completed a risk assessment for illegal content and half had completed an assessment to determine if children were likely to access their platform. Age assurance methods were also widely used, with most services setting minimum age requirements[12] and around half applying age assurance checks. However, only two in five were using age assurance methods identified in Ofcom's guidance as capable of being highly effective. User reporting and complaints processes were nearly universal, with multiple channels typically available and more than half saying they aimed to respond within 24 hours. Content moderation was similarly well established, with most services combining human and automated approaches.

- **Many of the services we spoke to had a named person responsible for conducting the required assessments and said they had completed at least one Online Safety Act-related risk assessment.** Almost three quarters (72%) of services had a named person responsible for conducting these assessments. Two thirds (67%) reported completing an assessment for illegal content and 53% reported completing an assessment to determine whether children are likely to access the service. Where a service is likely to be accessed by children it needs to conduct a risk assessment for content harmful to children. In total, 32% of all services we spoke to said they completed this assessment, typically within the past year.[13]
- **The majority of services reported having a minimum age requirement, although most stated they use an age assurance method that Ofcom has <u>not</u> to date identified as capable of being highly effective to enforce it.** The majority of services (79%) reported having a minimum age requirement. While 83% said they check the age of their users, this included services that relied on self-declaration, which is not regarded as age assurance under the Act. Overall, 41% reported using one or more age assurance methods capable of being highly effective, such as photo ID with a selfie, facial age estimation, or credit card checks. Among services with a minimum age requirement, 90% said they check users' ages, but fewer than half (45%) reported using one or more methods capable of being highly effective**.**
- **Almost all services (98%) had processes for users to report or make a complaint about content or behaviour that is in breach of their platform's policies.** The most common processes used were in-platform reporting tools (75%) and emailing a support team (75%). Over half (53%) of services stated that they aimed to action complaints within 24 hours.
- **The vast majority (94%) of services said they had content moderation processes in place and it was fairly common for services to use both human and automated processes (60%).**

[10] As mentioned above, reporting no changes in response to the Act does not necessarily indicate non-compliance, and the survey was not designed to assess whether changes were required.
[11] Please note: these results are based on a low base (n=27), comprising respondents who indicated they had not made any changes in response to the Act yet at the time the survey was undertaken.
[12] There is no requirement in the Act to set a minimum age limit or use highly effective age assurance to enforce any minimum age limit services choose to set. As per Section 12(11) of the Act provides that where regulated service providers use age assurance to restrict access to users under a certain age, they must enforce these age limits consistently to ensure children have age-appropriate experiences and are protected from harmful content.
[13] Note: the data is unable to identify those services likely to be accessed by children and therefore cannot identify which services would be required to conduct a risk assessment for content harmful to children.

Nine in ten (90%) services used human moderators, and two-thirds (64%) had adopted automated moderation tools.[14] The most commonly used automated processes were keyword detection (84% of those using automated moderation), rules-based or heuristic tools (75%) and AI/machine learning tools (61%).

4.4 Perceived barriers to implementation

Financial and resource constraints were commonly cited by services that had not yet made changes in response to the Act, with staff resource limitations also widely reported. Among those that had implemented changes, financial and labour impacts were most commonly cited, with around one in three claiming high or very high costs. Effort was concentrated particularly among regulatory/policy and technology teams.

- **Among those that reported not yet having made changes in response to the Act, the most commonly perceived barriers to implementation related to financial and staffing or resource constraints.** Other issues were mentioned by a minority as standing in the way of becoming compliant, including privacy concerns around age assurance.[15]
- **Those that said they had made changes in response to the Act tended to report financial and labour impacts.** Respondents were asked to rate costs in terms of how significant these were to their organisation, based on the following options and definitions: very low (costs were zero or near zero); low; medium (some opportunity cost in meeting the Act's requirements); high; very high (cost threatened the long-term viability of the organisation). **'**Medium' costs were most commonly cited, including labour costs associated with understanding and deciding how to comply with online safety regulation (44%), labour costs associated with making changes to the service (40%), and financial costs associated with making changes to the service (36%). While around one third claimed high or very high costs (33-36%), at least one in five claimed low or very low costs (20%-29%). Costs were highest for services that indicated their users had been exposed to illegal or harmful content or pornography services.
  - The qualitative research highlighted some of the costs involved: one business noted that they needed to increase their use of third-party platforms, which led to an integration cost of $30-50k and ongoing costs of $5-10k per month, another mentioned that they had to pay for external legal advice.
- **Labour costs tended to be concentrated among regulatory/policy and technology teams.**[16] Around half (51% and 49% respectively) of those who had implemented changes reported that these teams had spent a 'substantial' or 'very substantial' amount of time on their organisations' response to the Act. This compared with two in five (38%) saying content moderators had done so. The time spent by tech teams was more pronounced among businesses delivering 'pornography or reported risk' services, while regulatory/policy professionals and content moderators headquartered in North America were among those most likely to say they spend a 'substantial' or 'very substantial' amount of time implementing changes.

[14] Thirty per cent indicated that they only use human moderation and 4% that they only use automated processes, while 60% use both.
[15] Please note: these results are based on a low base (n=27), comprising respondents who indicated they had not made any changes in response to the Act yet at the time the survey was undertaken. As such we have reported these insights qualitatively.
[16] As above, these are subjective measures that rely on respondents' estimations. Respondents were asked how much time individual teams spent on working on their organisations' response to the Act and were given the following options: no time required; limited time; moderate amount of time; substantial amount of time; very substantial amount of time.

MRS Awards 2024 Winner Business Impact of the Year - UK
MRS Awards 2022 Finalist Business-to-Business Research
MRS Awards 2020 Winner Innovation of the Year
MRS Awards 2019 Winner Global Agency of the Year
MRS Inclusion Pledge

STRAT7 JIGSAW

Thank you

STRAT7 Jigsaw. A trading division of STRAT7 Limited
98 Theobalds Road, London, WC1X 8WB, UK
+44 (0)20 7291 0810

Web: www.jigsaw-research.co.uk
Email: info@jigsaw-research.co.uk

Registered in England no.: 7642707
Registered Address: 11 Soho Street, London W1D 3AD

VAT no.: 326 011 940

MAKING SENSE OF HUMAN COMPLEXITY