Categorisation

Advice submitted to the Secretary of State

Welsh overview available

Contents

Section

Annex

Overview

Ofcom is the United Kingdom's (UK) communications regulator, overseeing sectors including telecommunications, post, broadcast TV, radio, and online services. We were appointed the online safety regulator under the Online Safety Act 2023 (the Act) in October 2023.

The role of categorisation

All online services within scope of the Online Safety regime must protect all UK users from illegal content and, where applicable, protect children from online harm. In addition, a small proportion of these services will be categorised and designated as category 1, 2A or 2B services if they meet certain thresholds set out in secondary legislation by Government.

These categorised services will be required to comply with a range of additional requirements, largely focused on bringing an appropriate level of safety, transparency, and accountability to the online world, reflecting the nature of such services. This includes producing transparency reports, operating in line with terms of service, offering user empowerment tools, and preventing fraudulent advertising – depending on the category they fall within:

Categories →	Category 1	Category 2A	Category 2B
Categorised services must comply with additional duties relating to the below:			
Transparency reporting	☑	☑	☑
Enhanced requirements on risk assessments and record keeping	☑	☑	
Additional terms of service duties	☑		
Protections for news publisher and journalistic content, and content of democratic importance	☑		
Providing user empowerment features	☑		
Providing user identity verification options	☑		
Prevention of fraudulent advertising	☑	☑	
Disclosure of information about use of the service by a deceased child user	☑	☑	☑

What we were asked to do

Ofcom was required under the Act to carry out research and produce advice to the Secretary of State on the threshold conditions for each category of service, within six months of Royal Assent. **This document sets out the research we carried out and confirms our advice to the Secretary of State on categorisation, as required under the Act.**

How we carried out our research

The Act required Ofcom to carry out research on the threshold conditions for categories 1, 2A and 2B. The requirements for each category are set out in more detail in the body of this document.

Broadly, the Act required Ofcom to undertake research on a combination of service functionalities, user numbers, risk of harm, and any other characteristics that Ofcom deemed relevant.

We carried out our research between June 2023 and January 2024. We also published an open [Call for Evidence](#) in July 2023, inviting input from interested stakeholders. Our research involved a combination of analysing information submitted to Ofcom following the Call for Evidence, publicly available information, third-party datasets, pre-existing Ofcom research and new bespoke Ofcom research. Our main research sources were:

- **visitor reach data from Ipsos iris** – we analysed Ipsos iris data from October 2023 about UK internet users aged 15+ to inform research requirements on UK user numbers;
- **bespoke research on the functionalities of online services** – we undertook bespoke internal Ofcom research on the functionalities of in-scope online services to help inform the research requirements on functionalities; and
- **existing Ofcom research on risks of harm** – we drew on existing research, including some previously conducted or commissioned by Ofcom, to inform research requirements on the risk of illegal content or content harmful to children on relevant user-to-user and search services.

We set out more detail on our data sources and methodologies later in this document, including noting their limitations where relevant.

Our advice and proposed thresholds

The Act requires Ofcom to produce advice for the Secretary of State on where thresholds should be set, based on the research we have carried out. In completing our advice on categorisation, we have exercised our regulatory judgement having regard to our duties set out in the Communications Act 2003 and our functions under the Act.

> **What we are recommending to the Secretary of State – in brief**
>
> Our advice to the Secretary of State on proposed thresholds is as follows:
>
> **Category 1**
>
> Our research findings indicate that the features of a service most relevant to content being disseminated easily, quickly and widely are:
>
> - content recommender systems, because they are typically relied upon by services to amplify content to a wide set of users; and
>
> - the ability for users to forward or re-share content, because this facilitates users in sharing content instantaneously with others.
>
> In our view, these two features each operate to increase dissemination of content easily, quickly and widely. Additionally, the effects of these features are likely to be increased further as the user base increases and when these features operate in combination. In essence, the higher the user base, the more content that is likely to be shared.
>
> For these reasons, our advice is that category 1 thresholds should target services that fulfil either of the two following sets of conditions:
>
> Condition 1:
>
> - use a content recommender system; **and**
>
> - have more than 34 million UK users on the user-to-user part of the service, representing c.50% of the UK population.

Condition 2:

- allow users to forward or reshare user-generated content; **and**

- use a content recommender system; **and**

- have more than 7 million UK users on the user-to-user part of the service, representing c.10% of the UK population.

Category 2A

Our research findings indicate that service type is a relevant factor to the prevalence of illegal content and content that is harmful to children. Ofcom's draft risk assessment for illegal harms reports that vertical search services, i.e. search services that are only focused on a specific topic or type of content, present a lower-level risk of harm in comparison to general or general downstream search services, due to their limited search functionality. We therefore propose that thresholds for category 2A should not include vertical search services.

Our research indicates that search content that is illegal or harmful to children is accessible across a range of search services. It is also reasonable to conclude that the larger the number of users of a service, the greater the potential reach of search content.

For these reasons, our advice is that category 2A thresholds should target services that fulfil both of the following criteria:

- is a search service but not a vertical search service; **and**

- have more than 7 million UK users on the search engine part of the service, representing c.10% of the UK population.

Category 2B

Our research – largely based on our draft risk assessment for illegal harms – considered what functionalities play a key role in the dissemination of illegal content and content that is harmful to children. We have concluded that direct messaging is particularly relevant, as it allows a user to directly disseminate content to another user, without other users being able to see or access this content. We ruled out other potentially relevant functionalities.

We consider that a large user base is relevant to category 2B. The greater a service's user reach, the greater the risk posed by illegal content or content that is harmful to children. This is because more users may encounter illegal or harmful content or may be targeted by malicious users. As many category 1 services may also allow direct messaging, we are proposing a user number threshold which is lower than for category 1. This is to ensure that the category 2B thresholds capture an appropriate number of relevant – and distinct – services.

For these reasons, our advice is that category 2B thresholds should target services that fulfil both of the following:

- allow users to send direct messages; **and**

- have more than 3 million UK users on the user-to-user part of the service, representing c.5% of the UK population.

What happens next

The Secretary of State must consider this advice as part of determining the category 1, 2A and 2B threshold conditions to be set in secondary legislation. Once the secondary legislation has passed, Ofcom will then gather information as needed, including under our statutory powers to request information from regulated services. We will analyse the information gathered about services against the final thresholds and in accordance with the Act produce a published register of categorised services, and a published list of emerging category 1 services.

The published register of categorised services will determine which companies need to comply with the additional duties in the Act. Assuming secondary legislation on categorisation is finalised by summer 2024, we expect to publish the register of categorised services by the end of 2024. We are aiming to publish draft proposals regarding the additional duties on these services in early 2025. Over time, we will revisit and update our register of categorised services as appropriate.

We will shortly publish a Call for Evidence on the additional duties that apply to categorised services. We encourage services who think they may eventually be categorised based on this advice – and any other interested stakeholders – to read and respond to our Call for Evidence.

Our roadmap to regulation sets out our latest broader plans for implementation of the online safety regime.

1. Background

1.1   This section summarises the regulatory framework for categorisation under the Act, along with Ofcom's role in the process. Chapter 2 of Part 7 and Schedule 11 of the Act set out the process for how services will be categorised under the new regime.

The role of categorisation

1.2   All services within scope of the Online Safety regime under the Act are subject to duties in relation to illegal content and, where applicable, duties in relation to protecting children from harmful content.

1.3   Some regulated services will be designated category 1, 2A or 2B services under the Act if they meet certain thresholds set out in secondary legislation – we describe the framework for this below. These services will be required to comply with additional online safety duties, aimed at bringing an appropriate level of safety, transparency, and accountability to the online world, reflecting the nature of such services. This includes: duties to produce transparency reports; operating in line with terms of service; providing user empowerment tools; and preventing fraudulent advertising – depending on the category. Please see the table on page 3 above for a fuller list.

Regulatory framework

General duties

1.4   Ofcom is the independent regulator for communications services. We have regulatory responsibilities for communications, including the telecommunications, post, broadcasting, and online sectors. Ofcom's principal duty under the Communications Act 2003 is to further the interests of citizens in relation to communication matters, and the interests of consumers in relevant markets, where appropriate by promoting competition.[1] In performing our general duties, Ofcom is required to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed and any other principle appearing to us to represent the best regulatory practice.[2]

1.5   The Act formally appointed Ofcom as online safety regulator, with powers to implement and enforce the regime. In carrying out its functions, Ofcom is required to secure the adequate protection of citizens from harm presented by content on regulated service, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm. In doing so, it must have regard to (among other things): the risk of harm to citizens presented by regulated services; the need for it to be clear to providers of regulated services how they may comply with their relevant duties; and the need to exercise its functions so as to secure that providers of regulated services may comply with such duties by taking measures, or using measures, systems or processes, which are

---

[1] Section 3(1) of the Communications Act 2003
[2] Section 3(3) of the Communications Act 2003

proportionate to (i) the size or capacity of the provider in question, and (ii) the level of risk of harm presented by the service in question, and the severity of the potential harm.[3]

1.6 In completing our advice on categorisation, we have exercised our regulatory judgement based on our general duties and functions.

Categories of services

1.7 The Act makes companies that operate a wide range of online services (including user-to-user services, search services, and pornography services) legally responsible for keeping people, especially children, safe online. [4]

1.8 Certain regulated services will be designated as category 1, 2A or 2B services if they meet relevant thresholds set out in secondary legislation. These services will be required to comply with additional online safety duties where they meet certain threshold conditions. Different sets of threshold conditions will be set for each of the three separate categories of service. The Secretary of State will set these in secondary legislation, informed by research and advice provided by Ofcom.

1.9 **Category 1 services** are regulated user-to-user services that meet the category 1 threshold conditions. These must include at least one threshold condition relating to the number of users of the user-to-user part of the service, and at least one relating to the functionalities of the user-to-user part of the service. There may also be additional threshold conditions relating to other characteristics, if relevant. When setting threshold conditions, the Secretary of State must consider the likely impact of the number of users and functionalities of the user-to-user part of the service on how easily, quickly and widely content is disseminated on the services.

1.10 **Category 2A services** are regulated search services that meet the category 2A threshold conditions. These must include at least one threshold condition relating to the number of users of the search engine of regulated search services and combined services. There may also be additional threshold conditions relating to other characteristics of the search engine or factors relating to the search engine, if relevant. When setting these conditions, the Secretary of State must consider the likely impact that the number of users of the search engine may have on the level of risk of harm to individuals from search content that is illegal content or search content that is harmful to children.

1.11 **Category 2B services** are regulated user-to-user services that meet the category 2B threshold conditions. These conditions must include at least one threshold relating to the number of users of the user-to-user part of the service and at least one threshold condition relating to the functionalities of that part of the service. There may also be additional threshold conditions relating to other characteristics (as defined in the Act), if relevant. When setting these conditions, the Secretary of State must consider the likely impact that the number of users and functionalities of the user-to-user part of the service may have on the level of risk of harm to individuals from illegal content and content that is harmful to children disseminated by the service.

1.12 The Act states that the Secretary of State must specify the ways in which conditions may be met, and that may be by meeting the conditions in any specified combination subject two

---

[3] Sections 3(2)(g) and 4A of the Communications Act 2003.
[4] See Volume 1 of the Illegal Harms Consultation for more information on regulated services.

rules. Firstly, in relation to the category 1 threshold conditions and the category 2B threshold conditions, at least one specified condition about number of users or functionality must be met. Secondly, in relation to the category 2A threshold conditions, at least one specified condition about number of users must be met.

Key definitions relating to categorisation

1.13   We set out some key definitions below that we use throughout this document.

1.14   Broadly, a **user-to-user service** is an online service where users may encounter content (such as messages, images, videos, and comments) that has been generated, uploaded, or shared by other users. This includes services which allow direct messaging between users. Some specific service types are excluded from the regime.[5]

1.15   A **search service** is an internet service that is, or includes, a search engine, which enables a person to search some websites or databases. It does not include a service which enables a person to search just one website or database. [6]

1.16   A user-to-user service is a **regulated user-to-user service**, and a search service is a **regulated search service**, if the service **has links with the United Kingdom**, and it is **not otherwise exempt** by the Act.[7] For these purposes, a service is treated as having links with the United Kingdom if it has a significant number of United Kingdom users or such users form one of the target markets for the service (or the only target market). A service is also so treated if the service is capable of being used in the United Kingdom by individuals, and there is a risk of harm to individuals arising from content present on the service in question.

1.17   A **combined service** is a regulated user-to-user service that includes a public search engine. For the purposes of the regime, a "public search engine" means a search engine other than one in relation to which certain internal business service conditions are met.[8]

1.18   **User numbers** refer to United Kingdom users of the user-to-user part of a service or search engine.[9] For these purposes a 'United Kingdom user' may be either an individual in the UK or an entity formed in the UK. In either case, it doesn't matter whether the person is registered to use the service.[10]

---

[5] See Volume 1 of the Illegal Harms Consultation for more information on regulated services.
[6] Sections 3 and 229 of the Act.
[7] See Schedule 1 of the Act, which describe services that are exempt, including email, MMS, SMS and limited functionality services, services offering only one-to-one live aural communications, internal business services, and certain other services in the public sector, and the education and childcare sectors. See also Schedule 2 of the Act which describes services combining user-generated content or search content not regulated by the Bill with pornographic content that is regulated. There may also be a temporary exemption for those services notified as a Video Sharing Platform (VSP) under our VSP regime. However, this may not mean a full exemption where a service provider has notified a partially dissociable service. More information can be found on our website.
[8] This definition is set out in section 4(7) of the Act. The internal business service conditions are explained in paragraph 7(2) of Schedule 1 of the Act.
[9] Paragraph 5 of Schedule 11 to the Act.
[10] There are certain exemptions that apply where the person in question is acting in the course of business.

1.19   A **user-to-user part of a service** is, in relation to a user-to-user service, the part of the service on which content that is user-generated content in relation to the service is present.[11]

1.20   **User-generated content**, in relation to a user-to-user service, means content that is generated directly on the service by a user of the service, or uploaded to, or shared on the service by a user of the service, which may be encountered by one or more other users of the service by means of the service.[12]

1.21   **Regulated user generated content**, in relation to a regulated user-to-user service, means user-generated content subject to a list of exceptions that includes emails, SMS messages, MMS messages, and news publisher content.[13]

1.22   A **functionality** in relation to a user-to-user service includes any feature that enables interactions of any description between users of the service by means of the service.[14] A functionality in relation to a search service, includes (in particular) a feature that enables users to search websites or databases; and a feature that makes suggestions relating to users' search requests (predictive search functionality).[15]

1.23   For the purposes of categorisation, the **characteristics** of a user-to-user part of a service or a search engine part of a search service include its user base, business model, governance and other systems and processes.[16]

Preparing this advice

1.24   Ofcom is required by Schedule 11 to the Act to carry out research within six months of Royal Assent to advise the Secretary of State on the threshold conditions for each of the three categories based on its research.

1.25   To help prepare our advice, Ofcom published a Call for Evidence, requesting evidence and information from stakeholders to help inform the research requirements set out below. We carefully considered all responses as we prepared our final research and advice.

1.26   The Act sets out the broad parameters for categorisation, but in giving our advice it has also been necessary to rely on our own regulatory policy judgements, which we have exercised in line with Ofcom's general duties.

1.27   In developing our proposals, we have also taken into consideration the limitations of the research (as discussed in detail in Annex A1). In our own research methodologies, we have sought to account for differences in measurement between the available sources and key concepts as defined in the Act.

---

[11] Clause 211.
[12] Section 55(3) of the Act.
[13] Section 55(2) of the Act
[14] Section 233(1) of the Act.
[15] Section 233(3) of the Act
[16] Paragraph 6 of Schedule 11 to the Act.

Category 1

1.28 For category 1, Ofcom was required to carry out research into:

- how easily, quickly and widely regulated user-generated content is disseminated by means of regulated user-to-user services;
- the number of users and the functionalities of the user-to-user part of such services; and
- other characteristics or factors relating to the user-to-user part of such services that Ofcom consider to be relevant to category 1 threshold conditions.

1.29 Using our research, we were then required to recommend at least one threshold for the following conditions:

- number of users of the user-to-user part of the service; or
- functionalities of that part of the service.

1.30 We were able to recommend further thresholds in relation to any other characteristic or factor relating to the user-to-user part of the service that we considered relevant.

Category 2A

1.31 For category 2A, Ofcom was required to carry out research into the following aspects of the search engine part of regulated search services and combined services:

- the prevalence of search content that is illegal content and search content that is harmful to children;
- the number of users of the search engine; and
- other characteristics or factors that Ofcom consider to be relevant to category 2A threshold conditions.

1.32 Using our research, we were then required to recommend at least one threshold for the number of users of the search engine.

1.33 We were able to recommend further thresholds in relation to any other characteristic or factor relating to the search engine that we consider relevant.

Category 2B

1.34 For category 2B, Ofcom was required to carry out research into:

- the dissemination of illegal content and content that is harmful to children by means of regulated user-to-user services;
- the number of users and the functionalities of the user-to-user part of such services; and
- other characteristics that Ofcom consider to be relevant to the category 2B threshold conditions.

1.35 Using our research, we were then required to recommend at least one threshold for the following conditions:

- number of users of the user-to-user part of the service; or
- functionalities of that part of the service.

1.36 We were able to recommend further thresholds in relation to any other characteristic or factor relating to the user-to-user part of the service that we considered relevant.

Next steps

1.37   The Secretary of State must consider this advice when determining and establishing the categorisation thresholds in secondary legislation.

Establishing the register and emerging services list

1.38   As soon as reasonably practicable after the threshold conditions are set in secondary legislation, Ofcom must produce and publish a register covering each category of service.[17] We are also required to publish and maintain a list of 'emerging services', which are services that meet 75% of the category 1 user number threshold in addition to certain other threshold conditions that may be set out in the regulations. [18]

1.39   We expect to use our statutory powers to request information from a range of services to assess them against the thresholds set by the Secretary of State, entering each service that meets the relevant threshold to the corresponding part of the register. All services listed on the registers of category 1, 2A, and 2B services will then ultimately be required to comply with the relevant additional duties under the Act (see table above).

Maintaining the register and emerging services list

1.40   Once the register is published, Ofcom must maintain it on an ongoing basis.[19] We will keep it under review and update it as appropriate. If any of the threshold conditions are amended in secondary legislation, we will be required to re-assess the relevant entries on the register.

1.41   If a regulated service provider considers that its categorised service no longer meets the relevant thresholds, it may request Ofcom to remove it from the register, based on evidence. Service providers may also appeal Ofcom's categorisation decisions to the Upper Tribunal. This includes any decisions on which companies are categorised as 1, 2A and 2B as well as Ofcom's decisions to not remove services from the register on request from service providers.

Changing category thresholds

1.42   Once the first threshold conditions have been set, Ofcom may carry out further research – whether on its own initiative or in response to a request from the Secretary of State – for the purpose of advising the Secretary of State on whether the existing thresholds conditions remain appropriate.

1.43   The Secretary of State must consider any further advice from Ofcom and must publish a statement explaining any decision to depart from Ofcom's recommendation.

---

[17] Section 95 of the Act
[18] Section 97 of the Act
[19] Section 96 of the Act

2. Research methods and data sources

2.1   The research underpinning this advice has been collated using a combination of data sources and research methods. Here, we set out the research approach and key data sources that we have used in our research. **Ofcom's full analysis is laid out in Annexes A1 to A4.**

2.2   **The research relied on for the purposes of this advice is separate to the future process of designating services.** To compile the register of categorised services, Ofcom will seek to use its statutory information gathering powers to request the relevant information directly from services, including information about user numbers.

Our approach

2.3   Across the three categories, there are common areas that Ofcom was required to research, in particular in relation to the online services' user numbers and functionalities. Our approach to our research was informed by the four themes of consistency, objectivity, scope and transparency.

2.4   **Consistency**: Where possible, we have used the same sources of data and research across our work for all three categories to ensure consistency in our approach and findings. Our approach centred around two key data sources that address the cross-cutting research questions in relation to user numbers and functionalities. We also undertook or relied on additional research to address category-specific research questions.

2.5   **Objectivity**: To ensure that our recommendations were developed in a fair and impartial way, based on the available evidence, the datasets and insights generated through our research were completed in a service-agnostic way. Individual services were assessed at the outset for the purposes of mapping data relating to user numbers and functionalities. Our recommendations for threshold conditions were then developed and tested by reference to data compiled and analysed in a way that prevented individual services from being identified. Once our threshold proposals were developed, we reviewed these against a named list of services to understand the potential outcomes of our proposals. The details of how we conducted this process are laid out in Annexes A1 to A4.

2.6   **Scope**: We identified the need to use comprehensive and reliable data sources that, so far as possible, targeted a sizeable sample of services likely to be regulated under the online safety regime. We recognised at the outset that:

- There is no existing applicable, robust data on the criteria relevant to determining the threshold conditions for each category - in particular, in relation to UK user numbers on the user-to-user part of services, and functionalities. We therefore either used the best available data or created our own. Throughout our analysis, we have been clear about the known limitations of these approaches.
- To accommodate the online safety legal framework in our research, we would need to make a series of reasonable assumptions - based on publicly available information – to exclude services that were not likely to be within scope of the regulatory regime. These assumptions allowed us to generate a relevant, practical, and manageable set of data on which we could base our analysis.

2.7   **Transparency**: We have published the data that underpinned our research on user numbers and functionalities in Annex A1. Additional research sources that were used in the analysis are all publicly available and are also described in Annex A1.

Key datasets

2.8   The research we completed includes a combination of Ofcom's own analysis of publicly available information, Ofcom-commissioned research, and Ofcom analysis of third-party datasets.

2.9   The research questions differ for each category, which necessitated different methods. Despite this, there are some general, cross-cutting elements of our approach that underpin the research and ultimately the decision-making for our recommendations. We have been particularly mindful about ensuring a consistent approach to determining:

- **user numbers** (which arises in the case of each category);
- **functionalities** (which arises in the case of categories 1 and 2B, i.e., user-to-user services); and
- **other characteristics or factors that may be relevant** (which arises in the case of each category).

2.10   To deliver workable and transparent advice, we ultimately relied on two central, cross-cutting datasets to address the above criteria. In determining our recommendations, these were manipulated in different ways to answer category-specific research questions and test various policy proposals. The datasets are both limited to include services assessed to be likely in scope of the Act only. They do not include the names of individual services.

2.11   Given that the Act is a new regulatory regime, we relied on indicative assessments of services that are likely to be in-scope for the purposes of this research. We set out further detail on these steps in the research findings annexed to this advice.

Dataset 1: User numbers for user-to-user services, calculated using Ipsos iris UK visitor data

2.12   Ofcom was required to analyse the number of users of the user-to-user part of regulated user-to-user services as part of its research for category 1 and category 2B, and the search engine part of regulated search services as part of its research for category 2A.

2.13   Services define 'users' in varied ways, and this was confirmed in the responses we received to our Call for Evidence on categorisation. We also understand that services rely on varying methodologies to measure the number of users on their services.

2.14   We sought to identify a methodology that would allow us to consistently compare UK user numbers across services that are in scope of the Act. This kind of data is not typically made available by relevant services themselves. We concluded that the best data available to us regarding the UK reach of different online services within the UK's online population is the dataset available from Ipsos iris.[20]

2.15   There are important limitations to the use of this data as a proxy for assessing the number of UK users of a regulated service (or part of a service), which are noted in Annex A1. The key limitations are:
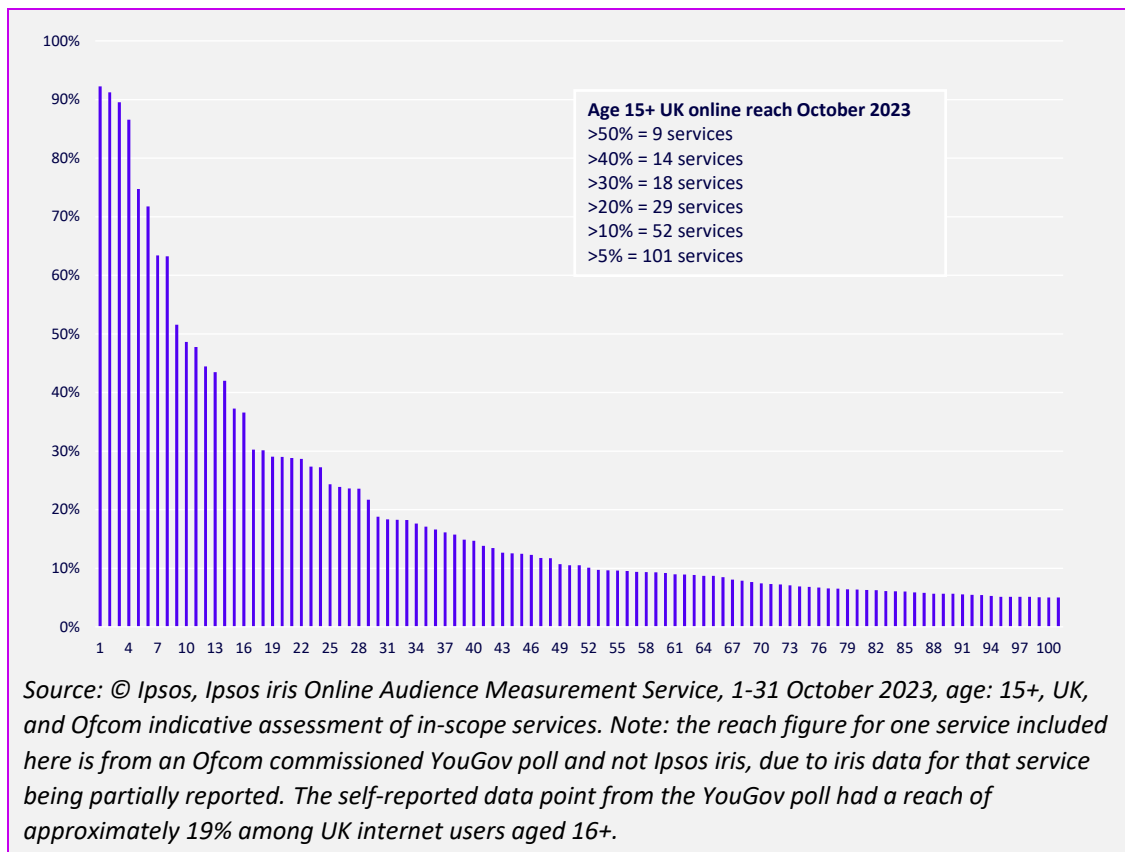
---

[20] Ipsos iris is an online measurement system, endorsed by UKOM as the UK standard for online audience measurement across PC, tablet and smartphone. More details can be found in Annex A1.

a) a brand/entity on Ipsos iris does not necessarily equate to a regulated service (or part of a service) under the Act;

b) Ipsos iris reach is modelled on a population of UK online visitors aged 15+ and therefore is not an exact measure of reach for the entire UK population; and

c) we have had to make indicative assessments of which services are likely to be in-scope of the Act for the purposes of creating a relevant database.

2.16 This data has only been used at this point for the purposes of producing research to inform Ofcom's advice on categorisation thresholds to the Secretary of State. To compile the register of categorised services, Ofcom will seek to use its statutory information gathering powers to request the relevant information directly from services, including information about user numbers.

2.17 We have relied on the most recent tranches of Ipsos iris data available for analysis at the time of writing, which is data covering the month of October 2023. Ofcom internal analysis of services likely to be in scope of the regime was combined with Ipsos iris data.[21] This produced a final dataset showing the **reach of UK online visitors aged 15+** on in scope user-to-user services, limited to those with a visitor reach of **5% or more of the UK online age 15+ population**.

Figure 1: Ranked UK visitor reach of likely in-scope user-to-user services with ≥ 5% UK online aged 15+ population reach in October 2023.

Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services. Note: the reach figure for one service included here is from an Ofcom commissioned YouGov poll and not Ipsos iris, due to iris data for that service being partially reported. The self-reported data point from the YouGov poll had a reach of approximately 19% among UK internet users aged 16+.

---

[21] We have conducted indicative initial scope assessments based on publicly available information on and about the services. Nevertheless, some services captured within the analysis, including retail services, may fall within the exemptions in Schedule 1 of the Act.

2.18   The full methodology for this dataset can be found in Annex A1, along with the underlying Ipsos iris data used, which is attached to this report as 'Dataset 4'.

Dataset 2: Dataset of relevant functionalities of likely in-scope user-to-user services

2.19   For our research for categories 1 and 2B, we were required to consider the functionalities of the user-to-user part of user-to-user services. We did not identify any existing independent assessments of the functionalities that different online services provide. This may stem from the lack of any widely adopted definitions for functionalities, as well as the regular changes that online services make to the functionalities they provide to their users.

2.20   Given this, Ofcom created a database of relevant online service functionalities that are offered by likely in-scope services for these purposes.

2.21   The services included in this dataset are the same as those included in Dataset 1. Namely, services had to meet two criteria to be included:

   a)   services had to have 5% or greater reach of UK online visitors aged 15+, as calculated using Ipsos iris data from October 2023; and
   b)   services had to be indicatively assessed by researchers as being likely to be in scope of the Act.

2.22   The provision of each functionality was labelled based on publicly available information from, and on, the relevant services. We accessed the online services to identify the functionalities provided.

2.23   We made an indicative assessment of each service for the presence of 22 functionalities.[22] These 22 functionalities were determined to be relevant to the category 1 or category 2B research questions. The research underpinning the selection of these 22 functionalities is available in Annexes A2 and A4. In short, the functionalities were selected for enabling (a) the easy, quick, and wide dissemination of content, as required for category 1 research or (b) the dissemination of illegal content or content harmful to children on user-to-user services, as required for category 2B research. The list includes:

   a)   one functionality which was identified as enabling content to be disseminated quickly, widely and easily;
   b)   six functionalities which were identified as enabling content to disseminate quickly, widely and easily as well as which were identified as key risk factors for the dissemination of illegal content;[23] and
   c)   15 functionalities which were identified as key risk factors for the dissemination of illegal content.

---

[22] We considered the role of content recommender systems as part of this exercise, reflecting the approach taken in Ofcom's previous work that considers 'functionalities and recommender systems' together, for example, in Ofcom's draft risk assessment for illegal offences, 'The causes and impacts of online harm'. References to functionalities here are to be construed accordingly. We note that the functionalities considered may not be mutually exhaustive.
[23] The six functionalities include five functionalities and content recommender systems which have been treated as a functionality for this exercise. Ofcom's initial research into functionalities that increase the risk of dissemination of content that is harmful to children (see Annex A4) identifies functionalities that are already included in this list of 22 functionalities. These include direct messaging, group messaging and content recommender systems.

2.24   The full list of functionalities and their definitions for the purposes of labelling are included in Annex A5.

2.25   Once labelled and quality assured, the names of individual services were redacted from the database and were replaced with high-level 'service type' descriptions. **This 'service type' version of the dataset was used for the purposes of developing recommendations for categories 1 and 2B.**

2.26   The service type labels we used were mostly taken from existing definitions published in Ofcom's first consultation, specifically in the draft risk assessment on illegal harms (Source 5). These definitions focus on the primary purpose of services rather than technical or functional specifics of how they work. They are, as such, quite general in nature and are only used in Dataset 2 for illustrative purposes. The service type labels allowed us to remove the names of services while preserving a sense of the type of services included in the dataset. We removed the names of services to ensure that the underlying logic and evidence base for our recommendations was fair and objective, but we included service type labels so that we could assess the workability and potential impact of threshold proposals as they were developed.

2.27   The full labelling methodology, quality assurance process and dataset limitations for Dataset 2 are outlined in Annex A1. The final 'service type' dataset used to inform policy recommendations is included as an attachment to this report, 'Dataset 2'.

Additional research sources

2.28   We also relied on other key sources for the purposes of our research. These additional sources are more particular to the category-specific research questions. Those sources are:

- Ofcom's 'Causes and Impacts of Online Harm', our draft assessment of online risks across the industry based on a literature review of nearly 1,000 sources.
- Ofcom's draft 'risk profiles', published in our first consultation on the illegal safety duties in the Online Safety Act. These risk profiles identify key risk factors that lead to a heightened risk of illegal activity or content on online services, based on our risk assessment (above). Key risk factors include specific functionalities of services.[24]
- Recently published Ofcom research on the risks of content harmful to children on online services, including reports about the risk of cyberbullying, self-harm, suicide and eating disorder content.
- Ipsos iris data from October 2023 showing the UK aged 15+ reach of search services.
- Ofcom and Ipsos's pilot children's passive measurement study on the internet use of 162 children aged 8-12 in the UK across smartphones, tablets, and computers.

2.29   The details of all research sources can be found in Annex A1.

---

[24] Both 'The causes and impacts of online harm' and 'risk profiles' were published by Ofcom in draft form for the purposes of consultation in October 2023. The final versions of these documents will be published as part of our statement in 2024.

3. Category 1 research and advice

Category 1 research and advice - in summary

Research: Our research findings indicate that the features of a service most relevant to content being disseminated easily, quickly and widely are:

- **content recommender systems**, because they are typically relied upon by services to amplify content to a wide set of users; and
- **the ability for users to forward or re-share content**, because this facilitates users sharing content instantaneously with others.

In our view, these two features each operate to increase dissemination of content easily, quickly and widely. Additionally, the effects of these features are likely to be increased further as the user base increases and when these features operate in combination. In essence, the higher the user base, the more content that is likely to be shared.

Advice: For these reasons, our advice is that category 1 thresholds should target services that fulfil **either** of the two following sets of conditions:

Condition 1:

- **the use of a content recommender system on its service; and**
- **have more than 34 million UK users on the user-to-user part of the service, representing c.50% of the UK population.**

Condition 2:

- **have a functionality that offers users the ability to forward or re-share user-generated content with other users of the service; and**
- **the use of a content recommender system on its service; and**
- **have more than 7 million UK users on the user-to-user part of the service, representing c.10% of the UK population.**

Key research findings

3.1   For category 1, Ofcom was required to carry out research into:

a) how easily, quickly and widely regulated user-generated content is disseminated by means of regulated user-to-user services;

b) the number of users and the functionalities of the user-to-user part of such services; and

c) other characteristics or factors relating to the user-to-user part of such services that Ofcom considered to be relevant.

3.2   The full methodology and findings of the research for category 1 are included in Annex A2.

How easily, quickly and widely regulated user-generated content is disseminated by means of regulated user-to-user services, considering the role of functionalities

3.3 We first carried out a literature review of factors that might affect content dissemination on user-to-user services. We found minimal existing research on the factors that affect or influence how 'easily, quickly and widely' content is disseminated. Some literature indicates that the size of the user base and service design (including functionalities and content recommender systems) might play a role in the size and rate of content dissemination, but there is not currently a consensus about the significance of separate elements, nor how they interact with one another.

3.4 We therefore carried out our own research into this topic. As part of our own research, we analysed the extent to which functionalities and other factors or characteristics allow user-generated content to be disseminated easily, quickly and widely on a service. In summary, our analysis found that a service having a **content recommender system** and/or one or more of **six discrete content-sharing functionalities** contributes to the easy, quick, and wide dissemination of content.

3.5 For the purposes of our research, we consider 'content recommender systems' to be algorithmic systems that, by means of a machine learning model or other technique, determine, or otherwise affect the way in which content (including user-generated content) is encountered by users of a service. We think they are especially relevant because they are typically relied on by services to facilitate user engagement with content by means of the service. Examples of products that use content recommender systems include text, image or video feeds that suggest content to users of a service.

3.6 In addition to having a content recommender system, we consider that having one or more of these six content-sharing functionalities contributes to the easy, quick and wide dissemination of content:

- Uploading or generating content without an account
- Forwarding or re-sharing user-generated content with other users of the service
- Forwarding or re-sharing user-generated content onto other internet services
- Livestreaming one-to-many
- Livestreaming many-to-many
- In-livestream chat

3.7 We think these six content-sharing functionalities are especially relevant because they facilitate users in uploading, generating or sharing user-generated content instantaneously or near-instantaneously, through a limited number of steps and with the potential to reach multiple users at once.

3.8 We analysed Dataset 2 to identify an indicative list of services that provide at least one of the six relevant functionalities or a content recommender system. We found these elements to be common among services with a reach of 5% or greater in the UK, with the three of elements most commonly provided among the 101 services being:

- Forwarding or re-sharing user-generated content on other internet services (61 services)
- Content recommender system (44 services)
- Forwarding or re-sharing user-generated content with other users of the service (31 services)

3.9   Thirty-seven services provide one of the six relevant functionalities and a content recommender system in combination. The types of service in Dataset 2 that provide at least one of the six relevant functionalities and a content recommender system are:

- Social media (11 services)
- Information-sharing (6 services)
- Pornographic services (5 services)
- Marketplaces and listing services (5 services)
- Video-sharing (4 services)
- Retail (2 services)
- Audio streaming (1 services)
- Gaming (1 services)
- Private communications (1 services)
- File-sharing (1 services)

3.10   Dataset 1 shows the distribution of visitor reach in the UK online aged 15+ population. Very few services have 40% reach or higher.

3.11   In general terms, the larger the user base of a service, the more widely content within that service can be shared. However, we note that platform policies can place limits on the breadth of sharing within a service, which is discussed in Annex A2.

Other characteristics

3.12   In carrying out our research, we considered a range of other characteristics such as business models, ownership, and size of services (in terms of employees and revenue). There was limited evidence that these characteristics are linked to how easily, quickly and widely content is disseminated.

3.13   Our research and the responses to our Call for Evidence on categorisation suggest that a service's policies can affect content dissemination. Policies that limit the potential audience of content, the activities of users or the duration for which content can remain accessible on a service each affect the potential breadth of content dissemination. These policies often differ within individual services and change regularly, however.

Advice on threshold conditions

3.14   In this section we set out the advice and recommended thresholds that Ofcom is required to provide to the Secretary of State for category 1. In this, we must recommend at least one threshold for the number of users, and at least one threshold for the functionalities, of the user-to-user part of user-to-user services.

3.15   Ofcom may recommend, if relevant, further thresholds in relation to any other characteristic or factor relating to the user-to-user part of user-to-user services.

3.16   We have also had regard to our recommendations relating to category 2B providers, which we discuss below. Categories 1 and 2B both relate to user-to-user services and refer to threshold conditions relating to functionalities and user numbers. We have therefore taken account of how each set of proposals may interact with one another (in the event they are adopted).

Discussion

3.17 In considering how easily, quickly and widely content is disseminated on user-to-user services, our research identified six functionalities and the use of a content recommender system as especially relevant (see above). This finding has formed the basis of our recommendation in relation to functionalities and other characteristics.

3.18 We analysed each of the six functionalities and content recommender systems and have concluded that two, in particular, stand out from our research as playing a particularly significant role in the dissemination of regulated user-generated content. These are:

a) **the use of a content recommender system; and**

b) **the ability to forward or re-share user-generated content with other users of the service**.

3.19 **Content recommender systems** amplify the breadth, scale and speed of content dissemination on a service by proactively disseminating content to new users or groups of users. Content recommender systems therefore play a fundamental role in enabling content to be disseminated easily, quickly and widely. **Forwarding or re-sharing existing content** with other users of a service is another key component of content dissemination, as it allows for the movement of existing content to new users or groups of users, by specifically enabling users themselves to affect content dissemination. These two features allow both the service and the user to affect the dissemination of content.

3.20 While our research indicates that the other functionalities identified were also closely related to how easily, quickly and widely user-generated content is disseminated, we consider that they did not play as core a role in content dissemination on user-to-user services. For instance, functionalities relating to livestreaming are relatively uncommon on the services considered in our sample. The ability to forward or re-share user-generated content across different online services may play a role in the dissemination of content between services but is not sufficient alone for content to be disseminated easily, quickly and widely, as this will depend upon the functionalities of the service to which content is forwarded.

3.21 We have also considered the relationship between the features identified above and the number of users of a service. There is no research available that indicates that there is a particular point at which the number of users has a marked or discernible impact on whether content is disseminated easily, quickly or widely. Rather, we think it is reasonable to assume there is a general trend indicative of content being disseminated with increased breadth as the number of users increases. In essence, the higher the user base, the more content that is likely to be shared. We therefore recommend taking an approach to category 1 that targets the largest services specifically.

3.22 Notwithstanding this, there are some noteworthy aspects to Dataset 2. Broadly, the services with the highest number of users are few in number and have similarly sized visitor numbers; the curve then sharply flattens and illustrates a relatively large number of similarly sized services with comparatively much fewer users.

3.23 Taking this into consideration, we judge that where services have a very large number of users, a content recommender system alone is sufficient for content to be disseminated easily, quickly and widely. This is because a service's content recommendation system results, in and of itself, in the dissemination of content to a very large audience without the need for users themselves to further share content.

3.24   Where services have a lower but still considerable number of users, a content recommender system alone may not be sufficient to disseminate content quickly, easily and widely. We judge that the ability for users to forward or re-share existing content on the service operates in conjunction with a content recommender to increase the likelihood of quick, easy and wide content dissemination: this can occur both through active content dissemination, driven by users' own engagement with content, as well as via content dissemination driven by the service's own systems.

3.25   Based on our analysis above, we therefore consider it appropriate to **recommend two sets of thresholds** for category 1.

3.26   We are required to recommend a user number threshold to the Secretary of State. In doing so we have exercised our regulatory judgement having regard to our general duties under the Communications Act 2003 and the function we are carrying out.

3.27   **Set one:** Considering the quick, easy and wide dissemination of content, we judge that services with content recommender systems and very large user bases are relevant to category 1. Based on our analysis, we propose that a user number threshold of 34 million UK users of the user-to-user part of the service is appropriate for such services. This represents approximately 50% of the total UK population.[25]

3.28   **Set two:** Considering the quick, easy and wide dissemination of content, we judge that services with content recommender systems, the ability for users to forward or re-share existing content on the service and large user bases are relevant to category 1. Based on our analysis, we propose that a user number threshold of 7 million UK users of the user-to-user part of the service is appropriate for such services. This represents approximately 10% of the total UK population.[26]

3.29   Our preliminary indicative analysis suggests that approximately 12-16 services may meet one or both of these user number thresholds, when factoring in the impact of the functionality requirements described above. This estimated number of services in our view indicates that our recommended user number thresholds are likely to strike the right balance in terms of targeting those services where content is likely to be disseminated easily, quickly and widely, while ensuring that the duties apply to a sufficiently targeted number of services.

3.30   We have discounted a recommendation that allowed for the categorisation of services by reference exclusively to functionalities and characteristics since the research indicates that user reach has an important role to play too. For instance, there are services where the functionalities and characteristics discussed above are core to the service, but whose smaller number base means that the dissemination of user-generated content on the service is comparatively less pronounced in its speed and breadth relative to other services with a greater number of users and the same functionalities.

3.31   We also considered the appropriateness of a recommendation that allowed for the categorisation of services by reference exclusively to user numbers but discounted this approach. A user component alone would not do justice to the findings from the research on functionalities and characteristics. For example, there are a number of services with

---

[25] Our approach to converting Ipsos iris data (which studies the UK online population aged 15+) into UK population thresholds can be found in Annex A7.
[26] Our approach to converting Ipsos iris data (which studies the UK online population aged 15+) into UK population thresholds can be found in Annex A7.

relatively large user reach, but whose services are primarily designed to facilitate limited and direct communication between a specified set of users, rather than being designed for the wide dissemination of content to a broad spectrum of different users.

3.32   For completeness, we considered whether the proposals should include other factors. We explored the merits of targeting the thresholds by reference to service type or business model (among other things), but the research did not highlight the existence of any other particular characteristics that play a notable role in the dissemination of regulated user-generated content easily, quickly and widely. We have therefore not included any further recommendations in respect of the threshold conditions for category 1. We are conscious that the regime remains in its infancy and there is nothing to preclude us from exploring these issues through our research in the future.

Proposed threshold conditions

3.33   To assist the Secretary of State in drafting the relevant legislation, here we provide more detail on how each element may be framed.

3.34   As discussed above, we judge it appropriate to recommend **two sets of thresholds** for category 1. We propose that services which meet **either** set one **or** set two would be categorised as category 1 services.

Proposed thresholds – set one

3.35   As to the **user numbers**, we believe that the legislation must codify certain principles that relate to the measurement of users to ensure that the threshold is sufficiently clear and transparent and provide a baseline level of consistency in approach. We discuss these principles in more detail in Annex A6. We therefore recommend a user number threshold condition for category 1 services to apply where the service has in excess of 34 million monthly users of the user-to-user part of the service, determined in accordance with the criteria set out in Annex A6.

3.36   As regards **other characteristics**, we recommend that a service must have a content recommender system. Our recommended definition of a content recommender system: 'An algorithmic system that, by means of a **machine learning model or other technique**, determines or otherwise affects the way in which content (**including user-generated content**) is encountered by users of a service. Typically, content recommender systems are relied on by services to facilitate user engagement with content by means of the service'.

Proposed thresholds – set two

3.37   As to the **user numbers**, we recommend a user number threshold condition for category 1 services to apply where the service has in excess of 7 million monthly users of the user-to-user part of the service, determined in accordance with the criteria set out in Annex A6.

3.38   As to **functionalities,** we are recommending that a service must have a feature that offers users with the ability to forward or re-share user-generated content with other users on the service. We consider 'forward' or 're-share' to relate to an ability to further share content that has already been uploaded to the service by a user. For clarity, we do not think the functionality of uploading needs to be captured in the legislative definition, as this is intrinsic to the functionality of forwarding or re-sharing user-generated content.

3.39   This concept is largely based on the reference in section s.233(2)(c) of the Act, the difference being that we are concerned expressly with user-generated content, a consequence of the fact that the research question relating to the ease, speed and breadth of content

dissemination was exclusively concerned with user-generated content. While we consider that it is important for this nuance to be reflected in the threshold conditions, we do not consider that the features should be excluded from falling within scope of this threshold condition if they also allow for the forwarding of other content (i.e., content that may not be user generated).

3.40   As regards **other characteristics**, we recommend that a service must have a content recommender system. We set out our recommended definition at paragraph 3.36 above.

<div style="border:1px solid #cc00cc">

Category 1 recommendation

We recommend to the Secretary of State that the regulations specifying conditions for the user-to-user part of regulated user-to-user services make provision that an entry relating to a service is added to the relevant part of the register established under subsection 95(2) OSA if:

Set one:

a) it has an average number of monthly UK users that exceeds 34 million, determined in accordance with Annex A6; and

b) in administering the user-to-user part of its service, it relies on a content recommender system, as defined in paragraphs 3.36 above

Set two:

a) it has an average number of monthly UK users that exceeds 7 million, determined in accordance with Annex A6; and

b) it includes any feature enabling a user to forward or re-share regulated user-generated content to other users on the service, accommodating the principles set out in paragraphs 3.38-3.39 above; and

c) in administering the user-to-user part of its service, it relies on a content recommender system, as defined in paragraphs 3.36 above.

</div>

4. Category 2A research and advice

<div style="background:magenta;color:white;font-weight:bold;padding:4px;">Category 2A research and advice - in summary</div>

Research: Our research findings indicate that service type is a relevant factor to the prevalence of illegal content and content that is harmful to children. Ofcom's draft [risk assessment](#) reports that vertical search services present a lower level of risk of harm in comparison to general or general downstream search services, due to their limited search functionality. We therefore propose that thresholds for category 2A should not include vertical search services.

Our research indicates that search content that is illegal or harmful to children is accessible across a range of search services. It is also reasonable to conclude that the larger the number of users of a service, the greater the potential reach of search content.

Advice: For these reasons, our advice is that category 2A thresholds should target services that fulfil both of the following criteria:

- **is a search service but not a vertical search service; and**
- **have more than 7 million UK users on the search engine part of the service, representing c.10% of the UK population.**

Key research findings

4.1 In accordance with our obligations under the Act for category 2A, we have carried out research into the following aspects of the search engine of regulated search services and combined services:

- the prevalence of search content that is illegal content and search content that is harmful to children;
- the number of users of the search engine; and
- other characteristics or factors that Ofcom consider to be relevant to category 2A threshold conditions.

4.2 The full methodology and findings of the research for category 2A are included in Annex A3.

The prevalence of search content that is illegal content and search content that is harmful to children

4.3 We reviewed what literature was available on prevalence of specific types of content on search engines. We found there is no established consensus on how to define or measure 'prevalence' in relation to harmful content on search engines. Prevalence is difficult to calculate on search engines as search engines can index an enormous amount of the web's content, and it is challenging to assess content at that scale to determine the proportional

presence of specific types of content. However, sampling methodologies can provide some indicative insights on overall prevalence.

4.4   Ofcom recently commissioned four research projects to analyse the risk of illegal content or content harmful to children being returned by search engines when users enter queries relevant to those harms. This collection of research found that potentially illegal content and content harmful to children can be accessed on search services used by UK users.[27] Potentially illegal content was accessible on all the search services studied in Ofcom's research, with no significant variations in the volume or prominence across the different search services that were tested. In relation to content that may be harmful to children, the largest sample study (see Source 4, Annex A1) assessed the availability of content relating to self-injurious behaviour: in this analysis, across all search services tested, over 1 in 5 results contained content which may be harmful to children out of over 37,000 search results analysed.

4.5   Our research found that a range of different search services have been used to access content that would amount to a range of offences, including terrorism, hateful content, extreme pornography, promotion of suicide and self-harm and child sexual abuse material (CSAM).

4.6   Our research did not establish a relationship between the number of users of a service and the prevalence of illegal search content and content that is harmful to children. However, we think it is reasonable to conclude – as with category 1 – that the larger the number of users of a service, the greater the potential reach of search content and therefore, also, of the subsection of content that may be illegal or harmful to children.

Other characteristics

4.7   We understand that there are three broad types of search services: general, general downstream and vertical.

   a) **General search** services maintain their own index and enable users to search for any listed website. They work by using automated processes designed to find and organise content (known as crawling and indexing). Algorithms are then used to rank the content based on relevance to the search query and other factors.

   b) **General downstream search** services provide the same function as general search services, but using an index that is purchased from a different organisation (namely a large general search service).

   c) **Vertical search services**, also known as 'speciality search engines', enable users to search for specific topics or genres of content, or products or services offered by third party providers. They operate differently from general search services. Rather than crawling the web and indexing webpages, they present users with results only from selected websites with which they have a contract, and an API or equivalent technical means is used to return the relevant content to users. Common vertical search services include price comparison sites and job listing sites.

---

[27] These research projects and a summary of their findings can be found in Annex 2. The full reports are available on the Ofcom website. Ofcom, 2024. One Click Away: a study on the prevalence of non-suicidal self injury, suicide, and eating disorder content accessible by search engines; Ofcom, 2023. Prevalence of potentially prohibited items on search services; Ofcom, 2023. Assessing the risk of foreign influence in UK search results; Ofcom, 2023. Online content for use in the commission of fraud - accessibility via search service.

4.8 We think that the type of search engine (i.e., general, downstream, vertical) has an impact on the likeliness of users encountering potentially illegal content or content that is harmful to children. Taking our recent research into account, we consider it is reasonable to conclude that general and general downstream search services are likely to pose risks to users in this regard. We consider that vertical search services – due to the specificity of their content (through searching select websites) and types of content that large vertical search services focus on - are less likely to pose risks to users in respect of encountering potentially illegal content or content that is harmful to children. However, we will monitor this issue in the future to see whether our view on potential risk changes based on evolving evidence.

4.9 In our consideration of other characteristics, our research found that some features of search services, such as autocomplete, Generative AI or predictive search capabilities, might affect the accessibility and prominence of potentially illegal content or content that is harmful to children. However, we did not identify any common sets of other characteristics that have an evident impact on the prevalence of illegal search content or search content that is harmful to children across different types of harm. Rather, the risks surrounding search characteristics differs for each type of illegal or harmful content studied. Ofcom will continue to conduct research into characteristics of search engines that might lead to increased risk of harm to users as part of its statutory functions. This will include consideration of any risks emerging from new technologies such as Generative AI, where they are deployed on search engines.

User numbers

4.10 We have considered the relevant user numbers. According to Ipsos iris, the UK search market is dominated by two services, one with 85% UK aged 15+ online reach and one with 43% in October 2023. UK reach figures to the two largest search services were specific to the 'search' sections of those brands, as determined by the Ipsos iris 'Search Engines' category. No other search service reaches more than 20% of UK internet users aged 15+.[28]

4.11 The most popular vertical search service has 16% UK online aged 15+ reach, followed by other vertical search services with 10% and 9% reach in October 2023. No other vertical search service included in this research had a UK reach greater than 5%. No general downstream search service had more than 3% UK online aged 15+ reach.[29]

---

[28] Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.
[29] Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

Figure 2: Ranked UK visitor reach of likely in-scope search services in the UK online 15+ population by search service type: October 2023
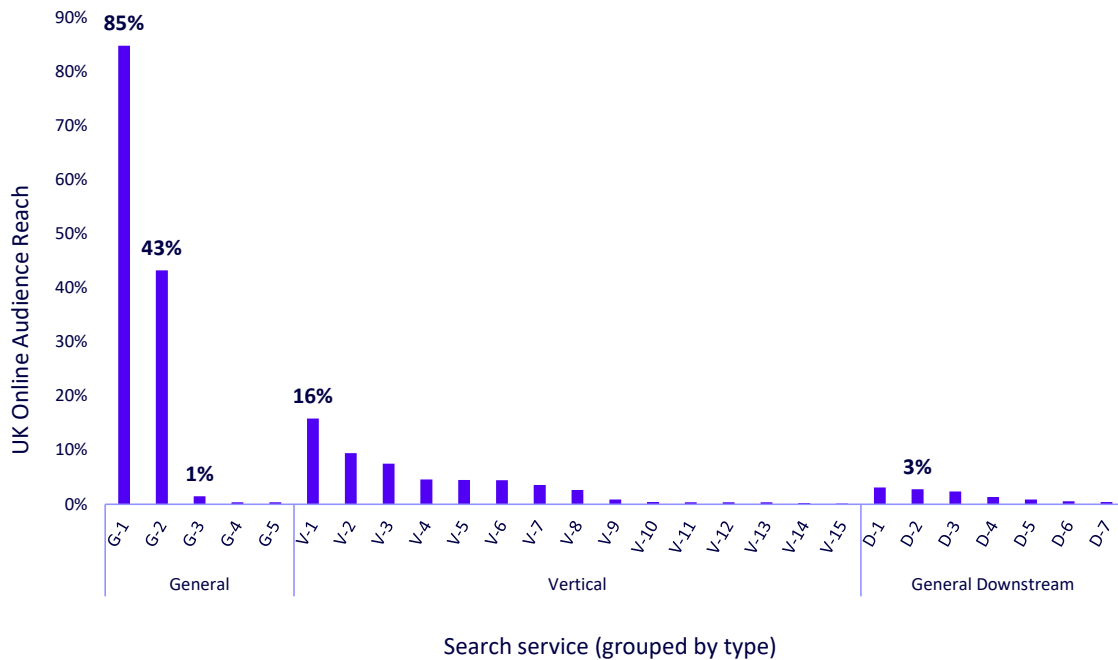
Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

Advice and proposed thresholds

4.12   In this section we set out the advice and recommended thresholds that Ofcom is required to provide to the Secretary of State for category 2A. For category 2A, Ofcom must recommend at least one threshold for the number of users of the search engine.

4.13   Ofcom may recommend further thresholds in relation to any other characteristic or factor relating to the search engine that we consider relevant.

Discussion

4.14   Our research, detailed above and in Annex A3, found evidence to suggest that potentially illegal content and content harmful to children is available and often easily accessible on a variety of search engines.

4.15   Our research did not establish a direct relationship between the number of users of a search service and the prevalence of search content that is illegal or harmful to children. However, as noted above, we consider it is reasonable to conclude that there is a correlation between the number of users of a service and the potential reach of search content that is potentially illegal or harmful to children.

4.16   We considered various service characteristics and factors but did not find sufficient evidence to support us proposing relevant thresholds in relation matters such as service features, business model, governance or systems and processes. Ofcom will continue to conduct research into characteristics of search engines that might lead to increased risk of harm to

users as part of its statutory functions. This will include consideration of any risks emerging from new technologies such as Generative AI, where they are deployed on search services.

4.17   We do however consider it appropriate to recommend that a threshold condition be set in relation to search service type. In recommending a user number threshold condition, we have exercised our regulatory judgement having regard to our general duties under the Communications Act 2003 and the function we are carrying out.

4.18   As noted above, we think that general and general downstream search services may pose risks to users in relation to being exposed to content that is potentially illegal or harmful to children.

4.19   In contrast, Ofcom's draft risk assessment (Source 5) reports that vertical search services present a lower level of risk of harm because vertical search services, unlike general or downstream search services, do not crawl the web and index webpages.[30] Instead, vertical search services present users with results only from selected webpages and so draw from a narrower, subject-specific, smaller pool of information. Based on this, we consider that there is unlikely to be a significant prevalence of illegal search content and content harmful to children on vertical search services. We therefore propose that thresholds for category 2A should not include vertical search services.

4.20   Our research did not identify a clear link between the number of users on a service and the prevalence of search content that is illegal or harmful to children. However, our research did identify that these types of search content are present on search services in general. In our view, search services with a large number of users have the potential to expose more users to illegal content or content that is harmful to children, should such content appear in search results. We therefore think that it is reasonable to conclude that there is a relationship between user numbers and their impact on level of risk of harm. For this reason, we consider the size of a service's user base to be a relevant factor when considering the prevalence of search content that is illegal or harmful to children, including the likely risk of harm – and that these need to be considered in setting thresholds for category 2A.

4.21   We considered the reach of relevant general and general downstream services. We have considered the potential impact of different user number thresholds on how many services would fall in scope.

4.22   Our analysis above indicates that there are currently two search services that have significantly higher reach than the rest of the market, followed by a longer tail of search services. There is currently a significant difference in online visitor reach between the two largest reaching search services (85% and 43% respectively) and other general or general downstream search services, with the third most-used general or general downstream service reaching 3% of UK users aged 15+.[31]

4.23   We note that the user bases of the two largest services represent a relatively high reach in terms of UK users, far exceeding the 10% reach threshold that we have proposed for category 1. Given the large gap in user base between the two largest services and the rest, we consider it important to not set a user number threshold so high that it could preclude

---

[30] Ofcom's 'The causes and impacts of online harm' and 'risk profiles' were published by Ofcom in draft form for the purposes of consultation in October 2023. The final versions of these documents will be published as part of our statement in 2024.
[31] Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

the inclusion of relevant services in the future. For this reason, we consider that an appropriate user number threshold to apply to category 2A services is 7 million UK users of the user-to-user part of the service. This represents approximately 10% of the total UK population.[32]

4.24 In exercising our regulatory discretion, we have chosen to target services where compliance with the relevant duties that apply to category 2A services will have the biggest user impact and avoid the risk of harm. Our preliminary indicative analysis suggests that two services may meet this user number threshold, when factoring in the type of search service. This estimated number of services in our view indicates that our recommended user number threshold is likely to strike the right balance in terms of targeting those services that present a higher risk, while not precluding the inclusion of other services that may present a higher risk in future, should their user base grow.

Proposed threshold conditions

4.25 Please see our recommendations under in Annex A6 in relation to how user numbers should be codified in legislation. Based on those principles, we recommend a **user number** threshold condition for category 2A services to apply where the service has in excess of 7 million monthly users of the search engine part of the service, determined in accordance with the criteria set out in Annex A6.

4.26 As to **other characteristics**, the component identified in our discussion above relates to the type of search service. In other words, we propose to exclude vertical search services from category 2A. Section 229 of the Act defines 'search engine' to include 'a service or functionality which enables a person to search some websites or databases (as well as a service or functionality which enables a person to search (in principle) all websites or databases); does not include a service which enables a person to search just one website or database.'

4.27 The Act does not distinguish between the different types of search engines. Ofcom has identified several types of search services based on the definitions in the Act and our understanding of how search services operate. For the purposes of proposing a threshold condition, we propose to define vertical search service as an internet service with a search engine that is only focused on a specific topic or genre of content.[33]

Category 2A recommendation

We recommend to the Secretary of State that the regulations specifying conditions for the search engine part of regulated search services make provision that an entry relating to a service is added to the relevant part of the register established under subsection 95(2) of the Act if:

a) it has an average number of monthly UK users that exceeds 7 million, determined in accordance with Annex A6; and

b) it is a search service but not a vertical search service.

---

[32] Our approach to converting Ipsos iris data (which studies the UK online population aged 15+) into UK population thresholds can be found in Annex A7.
[33] We note that this aligns with the discussion of search engines in paragraph 940 of the explanatory notes to the Act.

5. Category 2B research and advice

Category 2B research and advice - in summary

Research: Our research - largely based on our draft [risk assessment] - considered what functionalities play a key role in the dissemination of illegal content and content that is harmful to children. We have concluded that direct messaging is particularly relevant, as it allows a user to directly disseminate content to another user, without other users being able to see or access this content.

We consider that a large user base is relevant to category 2B. The greater a service's user reach, the greater the risk posed by illegal content or content that is harmful to children. This is because more users may encounter illegal or harmful content or may be targeted by malicious users. As many category 1 services also have direct messaging, we are proposing a user number threshold which is lower than for category 1. This is to ensure that the category 2B thresholds capture an appropriate number of relevant – and distinct - services.

Advice: For these reasons, our advice is that category 2B thresholds should target services that fulfil both of the following:

- **allow users to send direct messages; and**
- **have more than 3 million UK users on the user-to-user part of the service, representing c.5% of the UK population.**

Key research findings

5.1   In accordance with our obligations under the Act for category 2B, we have carried out research into:

- the dissemination of illegal content and content that is harmful to children by means of regulated user-to-user services;
- the number of users and the functionalities of the user-to-user part of such services; and
- such other characteristics that Ofcom consider to be relevant to specifying the category 2B threshold conditions.

5.2   The full methodology and findings of the research for category 2B are included in Annex A4.

Dissemination of illegal content and content that is harmful to children, considering the role of functionalities – and user numbers

5.3   We considered the evidence available on the dissemination of illegal content and content that is harmful to children.

5.4   As to **illegal content**, we recently consulted on our draft risk assessment (see Source 5) and draft risk profiles (see Source 6). This analysis considered what risk factors impact on the dissemination of illegal content. The research underpinning this found that direct messaging, encrypted messaging, and the ability to upload or generate content (videos and images) were the functionalities that play a key role in the direct dissemination of several different types of illegal content.

5.5   These functionalities were found to be key risk factors for the most number (7) of types of illegal harms that we considered as part of our risk assessment.

   a)   **Direct messaging**, also known as private messaging, is a user-to-user service functionality that allows a user to send and receive a message to one recipient at a time and which can only be viewed by that specific recipient. Evidence has found that direct messaging is used in the grooming of children, sharing of child sexual abuse material (CSAM), hateful content, controlling or coercive behaviour, intimate image abuse, fraud and harassment, stalking and threats offences. For example, perpetrators share illegal content with one another or commit and facilitate illegal offences via direct messages.

   b)   **Encrypted messaging** is a form of messaging that allows users to send and receive messages that are encrypted. Encrypted messaging is attractive to perpetrators due to a lack of moderation and reduced chance of detection. Encrypted messaging has been used in the perpetration of terrorism, grooming, CSAM, supply of drug and psychoactive substances, sexual exploitation of adults, fraud, and foreign interference offences.

   c)   **Allowing users to upload image or video content**[34] on open channels of communication, was identified as a key risk factor for the perpetration of terrorism, CSAM, promotion of suicide and self-harm, coercive or controlling behaviour, supply of drugs and psychoactive substances, extreme pornography and intimate image abuse offences.

5.6   As to content that is **harmful to children**, we will be consulting on our register of risks relating to the causes and impacts of content that is harmful to children in spring 2024. Our preliminary findings are that the following functionalities are a risk factor when it comes to encountering content that is harmful to children – direct messaging, the ability to upload and generate content (in particular, images and videos),[35] and content recommender systems. Our findings are not yet final.

5.7   We considered how commonly the functionalities noted above feature in Dataset 2. Our indicative view of the number of services that have these functionalities is set out below:

   a)   Direct messaging functionality is provided by 67 of the 101 services studied.
   b)   Encrypted messaging functionality is provided by between 12 and 32 of the 101 services studied.[36]
   c)   Uploading or generating image or video content functionality is provided by 77 of the 101 services studied.

---

[34] The draft risk assessment refers to this functionality as the ability to 'post content (images or videos)'.
[35] The upcoming risk assessment will refer to this functionality as the ability to 'post content'.
[36] Functionality labelling for encrypted messaging functionality was challenging to conduct using only publicly available information from or on services due to the lack of information provided by many services about the level of security provided on their messaging services. For this reason, 12 services were labelled as 'yes' for having encrypted messaging functionality and 20 were labelled as 'maybe' for this functionality provision.

5.8   We also considered the user base of relevant services. We ranked the 67 services that provide direct messaging functionality in Dataset 2 by their UK aged 15+ visitor reach. We found that 21 of these 67 services have a UK online aged 15+ reach of at least 20%.[37]

Considering the role of other characteristics in the dissemination of illegal content and content harmful to children

5.9   In carrying out our research, we considered a range of other characteristics, such as business models and commercial profile. There was limited evidence that these characteristics are linked to the dissemination of illegal content and harmful content to children.

5.10   Service type was also not found in our research to be an appropriate or workable characteristic for the purpose of recommending category 2B thresholds.

Advice on proposed threshold conditions

5.11   In this section we set out the advice and recommended thresholds that Ofcom is required to provide to the Secretary of State for category 2B. For category 2B, Ofcom must recommend at least one threshold for the number of users and at least one threshold for the functionality of the user-to-user part of a such a service.

5.12   Ofcom may recommend further thresholds in relation to any other characteristic or factor relating to the user-to-user part of such a service that we consider relevant.

5.13   We have also had regard to our recommendations relating to category 1 providers, discussed above. Categories 1 and 2B both relate to user-to-user services and refer to threshold conditions relating to functionalities and user numbers. We have therefore taken account of how each set of proposals may interact with one another (in the event they are adopted).

Discussion

5.14   We are required to recommend at least one threshold relating to the number of users of the user-to-user part of the service and at least one threshold condition relating to the functionalities of that part of the service. Our consideration of threshold conditions was informed by an understanding of the evidence about risk of harm, as outlined above.

5.15   Our research outlined above found certain functionalities that are involved in the dissemination of content and have been identified as key risk factors for several types of illegal content and/or content that is harmful to children. These are summarised as follows:

a)   **Illegal content**: direct messaging, upload or generate content (images and videos), and encrypted messaging.

b)   **Content that is harmful to children**: direct messaging, upload or generate content, and content recommender systems (although – as noted above – our findings are not yet final).

---

[37] Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

5.16   We consider these identified functionalities in turn – and whether we suggest they are included in the category 2B threshold conditions.

5.17   Our research suggests that the functionality of **direct messaging** is key to the dissemination of both illegal content and content harmful to children on user-to-user services. Direct messaging plays a key role in the dissemination of content from one individual user to another, in a manner that is not immediately accessible to, or known to, other users. Our evidence indicates that it is a factor strongly linked to various kinds of priority illegal offences including CSAM/CSEA, interpersonal threats such as harassment, stalking, coercive behaviour, and fraudulent activity that is reliant on transactions between individuals. Direct messaging was also identified in our research as playing a role in how children encounter harmful content such as cyberbullying.

5.18   For this reason, we recommend that category 2B thresholds relate to services which have the functionality of direct messaging, as it is a key factor in the dissemination of content that is both illegal and harmful to children.

5.19   **Encrypted messaging** was also identified as a key risk factor in the dissemination of illegal content in our research. Like direct messaging, encrypted messaging appears to enable the dissemination of content from one individual user or group to another, in a manner that is not immediately accessible to the service provider, who is therefore not in a position to moderate exchanges. Encrypted messaging provides additional layers of security for the users involved in the interaction by preventing the content from being accessed by any user, device, or entity outside of the intended recipient.

5.20   We considered whether it would be necessary to propose 'encrypted messaging' as a separate threshold. We are generally satisfied that any definition of direct messaging will by its nature capture both direct messaging that is encrypted, and direct messaging that is not. In relation to encrypted group messaging, we do not have sufficient evidence about how commonly services provide this specific subset of the encrypted messaging functionality to be able to recommend this as a threshold at this point in time.[38]

5.21   We considered whether it would be necessary to propose '**upload or generate content'** as a threshold, as this has been identified as a relevant functionality to the dissemination of both illegal content and content harmful to children. Our research found that the overwhelming majority of services in our dataset (91 of 101) offer the ability to upload or generate text and/or images and/or video content, and most of the services offer the ability to upload or generate image and/or video content (77 of 101). This suggests that the ability to upload or generate content by means of the service is a core enabler of user-to-user interaction and we therefore do not consider it necessary to set a threshold for 'upload or generate content'.

5.22   Finally, we considered **content recommender systems**. While these were identified as being relevant to the dissemination of content that is harmful to children, they were not identified through our research as a common key risk factor for the dissemination of different types of illegal content. As we have focused on content recommender systems in our category 1

---

[38] Functionality labelling for encrypted messaging functionality was challenging to conduct using only publicly available information from or on services due to the lack of information provided by many service providers about the level of security provided on messaging services. We did not separately assess whether services provide users with encrypted group messaging and/or encrypted 1-to-1 direct messaging, so we do not have evidence at this time to assess the appropriateness of recommending a specific threshold for group encrypted messaging.

thresholds, and because this feature has not been identified as one of the primary risk factors for the dissemination of both illegal content and content that is harmful to children, we consider it appropriate to not propose thresholds for content recommender systems for category 2B. This allows us to propose thresholds that create a distinct category that focuses on services where content is disseminated directly to users by other users, as opposed to category 1 where content is disseminated broadly, by means of the service.

5.23   Our research reported that content recommender systems pose a risk of disseminating content that is harmful to children specifically on those services that are used by children. We do not at this moment have sufficiently robust evidence about the services accessed by children of all ages to propose a threshold condition that would capture services that have content recommender systems that are specifically used by children. We therefore judge that setting a content recommender system threshold for category 2B could pose a risk of inadvertently capturing services that are not used by children and that therefore do not represent a high risk to either the dissemination of content harmful to children or content that is illegal. We also note that while we have limited data available on the services children use, Ipsos' child passive measurement pilot study (Source 10, Annex A1) indicated that the most visited services by online children aged 8-12 align closely with those of the adult online population.[39] The category 1 thresholds are therefore likely to apply to services that are also some of the services most accessed by children, which also have content recommender systems.

5.24   We next considered **user numbers**. In recommending a user number threshold condition, we have exercised our regulatory judgement having regard to our general duties under the Communications Act 2003 and the function we are carrying out.

5.25   We think it is reasonable to conclude that there is a correlation between user numbers, functionalities, and their impact on level of risk of harm by means of dissemination of content. The greater a service's user reach, the greater the risk posed by illegal content or harmful content, as there are more users liable to encounter such content, and a greater number of users who could be targeted by malicious users present on the service. With this in mind, we recommend targeting services with substantial user numbers under category 2B - although we need to bear in mind the relationship with category 1.

5.26   That said, category 2B services will only be required to comply with the duties relating to transparency reporting and disclosure of information about the use of the service by a deceased child user (which is arguably less onerous that the higher number of duties for category 1 and 2A services). Given these reduced obligations, we consider it is reasonable to set a lower threshold and capture services with a lower user base than categories 1 and 2A. However, we think the user reach needs to be substantial enough to ensure the benefits of the additional duties, such as transparency reporting, capture those services that present a sufficient risk.

5.27   Factoring in the proposed functionality threshold of direct messaging, we have considered the potential impact of different user number thresholds on how many services and service types would be in scope. We have also factored in the likely impact of our proposed category 1 thresholds.

---

[39] Ofcom Online Nation 2023, https://www.ofcom.org.uk/__data/assets/pdf_file/0029/272288/online-nation-2023-report.pdf

5.28   Our analysis suggested that many of the most-used services which have the functionality of direct messaging also met the category 1 thresholds, however a small number did not. As services will only be designated as one category of service, we are of the view that the user number threshold for category 2B must be lower than the user number threshold for category 1. This is to ensure that category 2B captures an appropriate number of different services to category 1. However, we found there are several high-reach services that have the functionality of direct messaging that do not meet the other proposed category 1 thresholds, so we consider it appropriate to not place an upper limit on the user number threshold (and capture those services where relevant).

5.29   Having assessed our research on the services that provide the functionality of direct messaging, we are proposing a user number threshold of 3 million users, which represents approximately 5% of the total UK population.[40]

5.30   Our preliminary indicative analysis suggests that approximately 25-40 services may meet this user number threshold, when factoring in the impact of the functionality requirements as described above. This estimated number of services in our view indicates that our recommended user number threshold is likely to strike the right balance in terms of targeting those services that present a higher risk, while ensuring that the duties apply to sufficiently targeted number of services.

5.31   Given the focus on the dissemination of content that is harmful to children, and the relevance of child users to a number of priority illegal harms, we explored whether it would be appropriate to propose additional user number thresholds in relation to children. Our research, as well as information received through our Call for Evidence, suggest that it is currently challenging for services to accurately identify and measure the number of child users. At this point in time we are therefore not recommending child user number thresholds, but this could be an area for future consideration.

5.32   Finally, we considered whether to recommend thresholds based on any other characteristics or factors. Our research did not highlight the existence of any other particular characteristics or factors that play a role in the dissemination of illegal content and content that is harmful to children. We weighed the merits of targeting the thresholds by reference to different types of users (by reference to criteria other than the number of users) or business model, among other things, but did not find compelling evidence to support doing so. We are conscious that the regime remains in its infancy and there is nothing to preclude us from exploring these issues through our research in the future.

Proposed threshold conditions

5.33   Please see our recommendations in Annex 6 in relation to how user numbers should be codified in legislation. Based on those principles, we recommend a user number threshold condition for category 2B services of 3 million or more UK users, determined in accordance with the criteria set out in Annex A6.

5.34   As to **functionalities**, we consider that direct messaging might be described for the purposes of this advice as a feature that allows a user to send content directly to, or receive such content directly from, another user on a part of the service.

---

[40] Our approach to converting Ipsos iris data (which studies the UK online population aged 15+) into UK population thresholds can be found in Annex A7.

5.35   We consider that a hallmark of direct messaging is that it has a private, or closed, component which means that content may only be exchanged (initially at least) on a part of the service where other users are unable to encounter it.

5.36   We note that 'direct messaging' is a functionality expressly mentioned on the face of the Act in section 233(2) and believe that aligns with what we describe above.

5.37   For completeness, we have not proposed threshold conditions for other characteristics or factors, for the reasons above.

Category 2B recommendation

In summary, we recommend to the Secretary of State that the regulations specifying conditions for the user-to-user part of regulated user-to-user services make provision that an entry relating to a service is added to the relevant part of the register established under subsection 95(2) of the Act if:

a) it has an average number of monthly UK users that exceeds 3 million, determined in accordance with Annex A6; and

b) allows users to send direct messages.

A1. Research and data sources

A1.1   This section outlines the data and research sources and associated methodologies used in Ofcom's categorisation research.

A1.2   The sources are organised by relevant category (1, 2A or 2B) apart from the two cross-cutting data sources that are used in research for multiple categories.

Cross-cutting data sources

Dataset 1: User numbers of relevant services, estimated using Ipsos iris data

Criteria for inclusion in the dataset:

- The entity had a UK online aged 15+ visitor reach of 5% or more in October 2023, according to Ipsos iris.
- The entity is assessed as a user-to-user service and as likely in scope of the Act by Ofcom researchers.

Data provider

- Ipsos iris is the UK Online Measurement (UKOM) endorsed currency for the measurement of audiences of online content of UK individuals aged 15+ who use the internet at least once a month. UKOM defines and governs the UK standard for audience measurement across computers, tablet, and smartphone. Ipsos iris provides data on UK aged 15+ visitor reach to apps and sites across smartphone, tablets and computers. For our research to inform categorisation advice, we have used Ipsos iris data from October 2023.

Ipsos iris methodology

- A passive single-source panel of over 10,000 adults who use the internet. Panellists install passive tracking software onto personally used digital devices (smartphones, computers, and tablets) which access the internet, with data collected continuously. The panel is recruited to be representative of the internet population demographically, geographically and by device type use.
- Census measurement of publisher websites and apps to collect visit measures for time spent and page views at a total level. Site-centric measurement involves placing on participating websites a short, device-agnostic JavaScript tag that identifies and logs all visiting devices. Similarly, app-centric measurement for mobile apps involves incorporating an SDK into the source code of participating applications. This logs the time of each app start event and the amount of time the app remains open, alongside details of event triggers which allow Ipsos iris to measure different behaviours within the app.
- A high-quality Establishment Survey, to produce universe targets. The Ipsos iris panel is then weighted to the internet population of UK individuals aged 15+ and demographic subgroups.
- External first-party data from accredited and approved sources with additional website or app level targets.
- Reporting on monthly data, all sources are fused together to create a synthetic dataset with more than one million records to represent the UK online infrastructure of websites

and apps. These can be analysed and reported at many demographic and geographic levels. As this is a synthetic dataset, it is not possible to provide confidence intervals/ranges for extrapolated population estimates. However, all extrapolated population figures provided are estimates that will have some margin of error. More detail on the Ipsos iris methodology can be found at https://iris.ipsos.com/what-we-offer/.

How Ofcom has used Ipsos iris data

- We identified the brands in Ipsos iris from October 2023 that had 5% or greater reach in the UK 15+ online population.
- Ipsos iris brands are not analogous with a 'service' or user-to-user part of a service, as defined in the Act. In the dataset, we have mainly assessed 'brand'-level entities, as listed in Ipsos iris. We looked at website-level and app-level data for service providers that we know to provide multiple services under the same brand, for example different websites and apps under the Google brand.
- We performed indicative scope assessments to identify which of those brands were likely user-to-user services in-scope of the Act. For this exercise, we developed an assessment matrix that listed factors that are laid out in the Act as exceptions (e.g. an internal business service or a recognised news publisher).[41] Analysts were provided with this matrix as well as an assessment guide for reference. Each analyst was assigned 10-20 services to assess. We double-assessed 20 of the services to support quality assurance of the data. Assessors received training on how to carry out an assessment. These assessments were made using information made publicly available by the online services.

Limitations for the purposes of categorisation research

- **Age**: Ipsos iris provides a measure of UK online visitors who are aged 15 or above. This does not include the portion of the UK online population that is aged 14 or below. We have conducted additional research (see Source 10) to try to fill some of these gaps in the measurement of UK users of relevant online services.
- **Population**: Ipsos iris is weighted to the internet population of UK individuals aged 15+, not the total UK population. Ofcom has produced additional analysis in its research below to compare reach statistics from the Ipsos iris population with equivalent estimates for the UK population as a whole. Please see Annex A7 for advice on the relevance of these details for proposed user number thresholds.
- **Small services**: Ipsos iris may not have reportable data on services with a very low number of UK visitors. If a service's associated websites or applications are tagged, then at least one panellist must visit the service in the given month for there to be reportable data. If a service's associated websites or applications are not tagged, then at least 20 panellists must visit the service in a given month for there to be reportable data.
- **Entity of measurement - services**: Ipsos iris does not use the same definition of an online service as the Act. Ipsos iris uses a hierarchy of measurable entities, including the Brand Group and its associated websites and apps. In some examples, a regulated service under the Online Safety Act may match a Brand Group or one of its websites or apps. In some cases, the regulated entity may not be specifically measured by Ipsos iris.
- **Number of users of the user-to-user part of services**: Ipsos iris data is not specific to the user-to-user parts of services. For some large services, Ipsos iris can provide data that is

---

[41] We have conducted indicative initial scope assessments based on publicly available information on and about the services. Nevertheless, some services captured within the analysis, including retail services, may fall within the exemptions in Schedule 1 of the Act.

specific to the website or application parts of those services. We used website or application specific data where it better reflects the user-to-user parts of those services.

Dataset 2: Dataset of relevant functionalities of likely in-scope user-to-user services

Criteria for inclusion in the dataset:

- The entity had a UK online aged 15+ visitor reach of 5% or more in October 2023.
- The entity is assessed as likely in-scope of the Online Safety Act by Ofcom researchers.

Methodology

Dataset 1 includes the most-used online user-to-user services in the UK that are likely to be in-scope of the Act (101 services, as of October 2023).

Analysts used publicly available information from the services to determine whether they did or did not provide a given list of 22 functionalities to their users. The list of functionalities was determined by analysis conducted for our research on categories 1 and 2B. This list includes:

a) one functionality identified as enabling content to be disseminated easily, quickly and widely;

b) six functionalities identified as both enabling content to disseminate easily, quickly and widely and identified as key risk factors for the dissemination of illegal content[42]; and

c) 15 functionalities identified as key risk factors for the dissemination of illegal content.

The analysis that led to the determination of these 22 functionalities can be found in Annexes A2 and A4. The definitions of these functionalities and the reasoning for their inclusion can be found in Annex A5.

Ofcom quality assured the labelling of the functionalities through a second round of coding. Analysts re-coded a sample of 22 of the 101 services for all 22 functionalities. Analysts also re-coded all 101 services for the 3 functionalities that are proposed as threshold criteria in the advice, namely 'sharing user generated content with other users of the service', 'a content recommender system' and 'direct messaging'. For both quality assurance processes, a third analyst made a final assessment where there was a discrepancy between the first and second round of labelling.

Once labelled and quality assured, the database was stripped of the names of individual services, which were replaced with high-level 'service type' descriptions. This 'service type' version of the dataset was used for the purposes of developing recommendations for categories 1 and 2B.

Service type labels are mostly taken from existing definitions published in Ofcom's first consultation, specifically in the draft risk assessment on illegal harms (Source 5). These definitions focus on the primary purpose of services rather than technical or functional specifics of how they work. They are, as such, quite general in nature and are only used in the Database for illustrative purposes. The service type labels allow us to remove the names of services while preserving a sense of the type of services included in the dataset.

We labelled services against these service type definitions based on publicly available information and our regulatory expertise. We quality assured the service type labels given to all 101 services

---

[42] The six functionalities include five functionalities and content recommender systems which have treated as a functionality for this exercise.

through a second round of coding, with a final decision-maker in place for any coding results with disagreement between the two initial rounds.

Service types include the following taken from Ofcom's draft risk assessment of illegal harms: Social media services, Payment services, Information-sharing services, Marketplaces and listing services, Video-sharing services, Gaming services, File-sharing services (referred to as File-storage and file-sharing services in the draft risk assessment), Private communications (referred to as Messaging services in the draft risk assessment).

We also included two other service types that were not included in the draft assessment of illegal harms and that we assigned definitions based on our regulatory understanding: Audio streaming services, Retail services. We also included Pornographic services as a service type, which was included in the draft assessment with a slightly different definition and called Adult services. The definitions for all service types can be found in Annex A8.

Dataset 5: User numbers of one relevant user-to-user service, estimated using YouGov data

Criteria for inclusion in the dataset

- The entity is assessed by Ofcom researchers and identified as a user-to-user service that is likely in scope of the Act.
- Fully robust audience data was not available for the one entity from Ipsos iris for October 2023.

Ofcom YouGov polls – Online Research Panels methodology

Ofcom works with YouGov Plc UK on the Online Research Panel project, which allows Ofcom to conduct online interviews administered to members of the YouGov UK panel of 2.5 million+ individuals who have agreed to take part in surveys. Emails are sent to panellists selected at random from the base sample. The email invites them to take part in a survey and provides a generic survey link. Once a panel member clicks on the link, they are sent to the survey that they are most required for, according to the sample definition and quotas. Invitations to surveys do not expire and respondents can be directed to any available survey. The responding sample is weighted to the profile of the sample definition to provide a representative reporting sample.

Fieldwork for the microblogging poll used here was undertaken between 6 and 11 September 2023, and the data can be accessed [here](#).

How Ofcom has used YouGov data

We used YouGov data from September 2023 to analyse the UK aged 16+ reported usage of the user-to-user service.

Limitations for the purposes of categorisation research

- **Survey data**: The data used is from an online survey where participants were asked to self-report their usage of this user-to-user service in the last month.
- **Age**: Whereas Ipsos iris data measures the 15+ online population, the total sample for the poll used here is weighted and representative of UK internet users aged 16+ only.

Category 2A: Data sources

Dataset 3: User numbers of relevant search services, estimated using Ipsos iris reach data

Criteria for inclusion in the dataset

- The entity is assessed by Ofcom researchers and identified as a search service that is likely in scope of the Act.[43]

How Ofcom has used Ipsos iris data

- For details of the Ipsos iris methodology, see Dataset 1 (above).
- We used Ipsos iris data from October 2023 to analyse the UK aged 15+ reach of search services.
- Ipsos iris 'brand'-level entities are not analogous with a 'service' or the search engine part of a service, as defined in the Act. In the dataset, we mainly assessed 'brand'-level entities, as listed in Ipsos iris. For some search services, however, we analysed UK visitor reach to the 'search' sections of those brands, as determined by the Ipsos iris 'Search Engines' category. This allowed us to analyse data that better reflects the visitor reach of the search engine part of those services, where that data was available in Ipsos iris.

Limitations for the purposes of categorisation research

The same limitations to the use of Ipsos iris data for the purposes of categorisation research that are described in Dataset 1 apply here, in addition to the following:

- Number of users of search engine part of services: Ipsos iris data is not specific to the search engine part of services. For some search services, Ipsos iris can provide data that is specific to the search 'section' of those brands, as determined by the Ipsos iris 'Search Engines' category. We used data specific to the search section of brands where it was available in Ipsos iris, and where it better reflects the search engine part of those services.

Data on the dissemination of illegal content and content harmful to children on search services

Source 1: Online content for use in the commission of fraud – accessibility via search services

Type of Harm

Illegal Harm - Fraud (specific offence = making or supplying articles for use in frauds)

Search services included in the research

Google Search; Bing Search

Description of research

The research involved searching for fraud-related products and information on major search services and assessing the content (the search result and the corresponding webpage) returned in the first 20

---

[43] The list of search services we analysed came from services listed as 'Search Engines' by Ipsos iris, which we internally reviewed to assess whether they would be likely to be in scope of the Act, as well as other services identified as potential search services by other internal projects at Ofcom.

search results for each search query, to determine if it could be considered 'likely to be prohibited' (i.e. meeting criteria developed specifically for the research that suggest the content could amount to an offence of making or supplying articles for use in frauds).

Key findings

[Existence] Is illegal content shown in search content?

- Content offering to supply articles (information or items) for use in the commission of fraud was easy to find and prevalent in samples tested on Google Search and Bing Search.

[Prominence] Is illegal content shown in the first 2 pages of results?

- Search queries tested returned large volumes of 'likely to be prohibited' content within the first 20 search results. This was as high as 100% of results shown on the search engine's search results page for certain queries; and 90% of the corresponding webpages that these search results led to (please note that some webpages could not be viewed).
- In 9 of the 11 search queries tested, 'likely to be prohibited' content appeared within the first three search results.

[Prevalence] What is the scale of this illegal content?

- The overall volume of this type of content or how often it is accessed or used to commit fraud could not be determined from this research.
- Within the first 20 results among the sample in this study, prevalence of this content was high. But the volume within the whole search index cannot be known.

[Please note: the search queries tested were intended to surface this kind of content if it existed within the service's index and would be considered relevant by the rating and ranking system that service uses to order search results.]

Other key findings

- 'Likely to be prohibited' content appeared in sponsored results/ads on Google Search and Bing Search
- 'Autocomplete' and 'Related searches' functions provided the user with additional search queries that would return 'likely to be prohibited' content
- Links to dark web sites appeared within the search results

Source 2: Assessing the risk of foreign interference on search services

Type of Harm

Illegal harm - Foreign Interference

Search services included in the research

Google (Search and News), Bing (Search and News), Yandex and Baidu

Description of research

Ofcom commissioned the Alliance for Securing Democracy to carry out research into how forms of manipulation or interference (which may meet the threshold for the Foreign Interference Offence) could take place via online search services.

Key findings

[Existence] Is illegal content shown in search content?

- The research did not attempt to make a judgement on the illegality of content, rather identify a potential risk of foreign interference by determining the types of variables that regularly generate search results from state-linked websites. However, it did pay particular attention to the presence of content produced by foreign state-backed media outlets currently sanctioned by the UK Government, such as RT.

[Prominence] Is illegal content shown in the first 2 pages of results?

- Data was collected from the first four pages of search results for each search term for all search services except Yandex, where results were limited to roughly one page due to platform limitations. The research found that links to RT and Sputnik typically appeared halfway down the second page of results on Google and Bing.

[Prevalence] What is the scale of this illegal content?

- On Google Search, Google News, Bing and Bing News, there were 23,756 observations of websites that were determined to have direct or indirect links directly or indirectly to a foreign state during the research period, with state-backed media representing 2.7% of all results. Overall:

> Yandex Search: Close to 27% of all results came from state-backed media outlets;
> Baidu Search: 6% of results came from state-backed media outlets;
> Google News: 4.2% of results came from state-backed media outlets;
> Bing News: 3.2% of results came from state-backed media outlets;
> Google Search: 2.4% of results came from state-backed media outlets;
> Bing Search: 1.2% of results came from state-backed media outlets.

[Note: search queries were, in part, chosen due to their potential to be weaponised by hostile foreign powers].

Other key findings:

- Sanctioned Russian state-backed media outlets: These were largely not present on search products owned by Microsoft and Google, with most returns for Russian state-media outlets on these platforms coming from non-sanctioned outlets like TASS.
- Impact of the design of search queries: Differences in the spelling, language and framing used in search queries had a large impact on search results. For example, using the Russian spelling "Kiev" produced 10-times more results from state-backed sources on Microsoft and Google-owned search products than when using the Ukrainian spelling "Kyiv".

Source 3: Presence of potentially prohibited items on search services

Type of Harm

Illegal harm - drugs and psychoactive substances, firearms and other weapons

Search services included in the research

Google, Bing and DuckDuckGo (additional hypotheses only)

Description of research

Ofcom commissioned PUBLIC to provide us with an evidence base regarding the ease of access and prevalence of content that contains an apparent offer to sell or supply a range of potentially prohibited items on search services. These items spanned four categories: knives and bladed weapons, firearms, controlled drugs, and psychoactive substances. We conducted 384 searches, each one seeking to identify how many webpages within a limited sample could be classified as

meeting the criteria for containing potentially prohibited content (PPC). Websites were classified as containing PPC when they met three criteria: the presence of a potentially prohibited item as a product; the presence of a clear route to purchase; and accessibility to a UK resident. This is an indicator of likelihood, rather than direct evidence of an offence being committed.

Key findings

[Existence] Is illegal content shown in search content?

- The research found webpages classified as containing PPC within the sample of URLs reviewed for every item/substance tested across Google and Bing. Searches for psychoactive substances retuned the most webpages classed as containing PPC, and searches for firearms returned the fewest. All webpages classified as containing PPC could be accessed in "one click" from the search engine results page.

[Prominence] Is illegal content shown in the first 2 pages of results?

- The research focused on the first three pages of search engine results and found that webpages classed as containing PPC tended to appear high up on the results page. More URLs classified as potentially prohibited content came from search results 1-10 (i.e. the first page), compared to either 11-20 (second page) or 21-30 (third page).

[Prevalence] What is the scale of this illegal content?

- Of the four search service products tested (text, image, video, shopping), text search returned the highest number of webpages classed as containing PPC, at 115 out of 1152 pages reviewed.
- The category of search queries that returned the most webpages classed as containing PPC was psychoactive substances – the sample of 1152 search results reviewed contained 63 webpages that were classified as containing PPC. However, these figures should be taken as nothing more than indicative – they represent a specific point in time and are a snapshot of search results from the fieldwork (April 2023).

Other key findings

- Functionalities: The research found that autocomplete, the search product used (i.e. text, image, video, shopping), related and sponsored searches were functionalities that played a role in surfacing PPC identified in the sample.
- Search query type: The research also found that using an extended search query, a query containing coded language, targeted slang or purchasing-related language, returned greater numbers of webpages classed as containing PPC than more general forms of search query.

Source 4: Prevalence of self-injurious behaviour on Search

Type of Harm

Content that is harmful to children - Non-Suicidal Self-Injury, Suicide, and Eating Disorders (SHED)

Search services included in the research

Google, Bing, Yahoo, DuckDuckGo and AOL.

Description of research

A quantitative assessment on the prevalence and accessibility of SHED content on five search services. Researchers inputted relevant keywords into the search services studied and manually coded the search results (over 37,000 results) to determine whether they contained content that is harmful to children. The coding schema included categories for content that: encourages others to

engage in self-injurious behaviour; glorifies or celebrates self-injurious behaviour; focuses on providing help, support or education; is ambiguous as to whether they sought to prevent or promote self-injurious behaviour; is irrelevant. The research also examined other factors such as how high the results appeared in search rankings, trends related to the results returned for different types of keyword queries, and differences in types of content (image, text).

Key findings

[Existence] Is content harmful to children shown in search content?

- Content that is harmful to children appears in search results. Harmful eating disorder content was the most prominently displayed of the various types of harmful content assessed across search services, with the exception of Google, where self-harm was the highest ranked on average.

[Prominence] Is content harmful to children shown in the first 2 pages of results?

- Items of content harmful to children (content that celebrates, glorifies or instructs self-injurious behaviour) often appeared on the first page of results.
- Across search services, SHED content is easily accessible and often appears on the first page of search results.

[Prevalence] What is the scale of this harmful content to children?

- Across all search services, out of 37,647 results analysed, over 1 in 5 results contained content which may be harmful to children (instructs, glorifies or celebrates self-injurious behaviour).
- There was no notable difference in prevalence of this kind of content between different search services studied.
- In 37,647 individual search result links across all five search services, we found that 22% of links contained content that celebrates, glorifies, or instructs self-injurious behaviour. All of this content was available in a single click ('one click away') from the main search engine page results.

Other key findings

- 50% of content that was coded as containing content that is harmful to children came from image search results.
- Content classed as likely to be harmful to children was often linked to coded terms and slang.
- Almost 60% of content classified as instructing, glorifying or celebrating self-injurious behaviour came from three social media domains.

Category 2B: Data sources

Source 5: Ofcom draft risk assessment for illegal offences, 'The causes and impacts of online harm'

As part of its duties under the Act, Ofcom produced an assessment of the evidence of risks of harm by illegal content on user-to-user and search services. The draft of this analysis was published as part of Ofcom's first consultation on the illegal safety duties under the Act in November 2023, "The causes and impacts of online harm". This analysis examines where and how illegal harms manifest online and the factors that give rise to risks of harm.

Methodology

Ofcom's risk assessment focuses on the over 130 priority offences defined in the Act. Ofcom's risk assessment considered priority offences and priority illegal content, which include terrorism offences, offences related to CSEA and other priority offences. These are detailed in Online Safety Illegal Harms Consultation Annex 5: Service Risk Assessment Guidance. So-called 'inchoate offences' are also treated as priority offences. These are grouped into several kinds of illegal harm. These include illegal harms such as: Child Sexual Exploitation and Abuse (CSEA), terrorism, fraud and hateful content. The risk assessment included analysis of nearly 1,000 sources of research and data. The range of material included in the risk assessment analysis includes relevant Ofcom research, academic papers from a range of disciplines, reports from government bodies, third-party sources and information from charities and other non-government organisations.

Limitations for the purposes of categorisation research

Ofcom's draft risk assessment for illegal offences considered both the presence of illegal content on user-to-user and search services, as well as the use of user-to-user services to commit or facilitate priority offences. As such the findings of the risk assessment, used in this research, go beyond dissemination of illegal content, but also include how service characteristics are used and enable offences to be committed online.

Ofcom's draft risk assessment of the causes and impacts of online harm to children is due to be published in spring 2024. Therefore, for research questions relating to the risk of content that is harmful to children on relevant services, we have relied on Ofcom-commissioned qualitative research produced in 2023. We have analysed the findings from Ofcom research studies, looking at cyberbullying, violent content online and content related to eating disorders, self-harm and suicide. We assessed the findings of these studies to identify any evidence of risk factors that are associated with a heightened risk of content that is harmful to children being disseminated on user-to-user services. Ofcom is consulting on its draft risk assessment and the final version may change based on the consultation responses received.

Source 6: Functionalities that are key factors for illegal offences – Ofcom's draft risk profiles

The Act requires Ofcom to prepare and publish 'Risk Profiles' based on the findings in our risk assessment (see Source 5). Ofcom has produced a set of draft Risk Profiles that outline the key factors that we consider are associated with a heightened risk of illegal harms, based on the assessment of evidence compiled in the draft risk assessment. The risk profiles include a selection of service characteristics (such as user base, business models and functionalities).

Methodology

In its work to develop the risk profiles, Ofcom conducted a qualitative analysis to identify which risk factors identified in the risk assessment (Source 5) were most strongly associated with the different kinds of illegal harms (i.e. key risk factors). We determined that a qualitative methodology was better able to provide an accurate assessment of the evidence base available given the complexity of the evidence and the lack of consistent or comparable quantitative data across and within harm types. The methodology considered: the strength of the evidence for different risk factors; how integral the risk factor was to an offence occurring; to what extent a risk factor makes it easier for an illegal offence to occur; and to what extent a risk factor increases the number of individuals exposed to illegal content.

There are a number of illegal offences for which there is minimal evidence about what creates risk of harm.

There is no consistent and comparable data to measure the risk created by different functionalities on different services for different illegal offences. The assessment of which risk factors are 'key' risk factors is therefore a qualitative assessment based on the best available evidence. Our analysis for categorisation has involved quantifying this qualitative assessment to identify the functionalities that should be considered for thresholds. This approach has its inherent limitations and reduces the depth of understanding of risks online but it has been done to allow us to try and compare the role of functionalities in the dissemination of illegal content.

Due to size of the risk assessment, our categorisation analysis does not take into account every risk factor identified for each kind of illegal harm (as assessed in Source 4). Instead, our analysis for categorisation has prioritised the key risk factors outlined in the risk profiles.

Ofcom is consulting on its draft risk profiles and the final version may change based on the consultation responses received.

Source 7: Key attributes and experiences of cyberbullying among children and young people in the UK[44]

The National Centre for Social Research (NatCen), in partnership with City University and supported by the Anti-Bullying Alliance and The Diana Award, was commissioned by Ofcom to undertake qualitative research to understand key attributes and experiences of cyberbullying among children in the UK. The research aimed to explore four primary research questions: what does cyberbullying look like among children?; what are the pathways for children being exposed to cyberbullying?; what impacts does cyberbullying have on children? ; and, what works to address cyberbullying?

The project consisted of three stages of research:

- One-to-one interviews with 10 practitioners with self-reported experience supporting children who had experienced cyberbullying.
- Qualitative research in six secondary schools across England, Wales and Scotland. This included paired or triad interviews with 14 members of school staff, and 12 focus groups with 50 children (aged 12-16).
- One-to-one interviews with 12 children with direct experience of cyberbullying (aged 14-17).

Source 8: Experiences of children encountering online content promoting eating disorders, self-harm and suicide[45]

Ofcom commissioned Ipsos UK and TONIC to conduct qualitative research to understand the pathways through which children encounter online content that promotes, glamourises or romanticises suicide, self-harm and eating disorders. There is currently limited understanding of how children encounter this type of harmful content online. This research sought to build on the current evidence base by further exploring online content that professionals, children and young people, perceive to promote suicide, self-harm and eating disorders, perceptions of how harmful this

---

[44] The research will be published on the Ofcom website on 13 March 2024.
[45] The research will be published on the Ofcom website on 13 March 2024.

content can be and the impact it has on children. Pathways to encountering this content and perceptions of mitigations to prevent children from encountering this content were also explored.

The research included a scoping phase and mainstage interviews. The scoping phase involved consulting with children and young people and professionals to inform the design of recruitment and research materials, including the ethical and safeguarding procedures, and was underpinned by trauma informed fieldwork processes. The mainstage involved 17 interviews with children and young people aged 13-18 years old who had encountered online content which they considered promoted suicide, self-harm or eating disorders (core sample) and also with children and 14 young people aged 13-21 years old with lived experience of suicidal ideation, self-harm and eating disorders, anxiety and depression, who had encountered online content which they considered promoted suicide, self-harm or eating disorders (lived experience sample). 10 Interviews were also conducted with a range of professionals with a safeguarding responsibility as part of their role and with first-hand experience of working with children who have encountered eating disorder, self-harm or suicide content online.

Source 9: Understanding pathways to online violent content among children[46]

Family Kids & Youth were commissioned by Ofcom to explore the pathways through which children encounter violent content online, and research was carried out between May – November 2023. The research had three stages: 2 focus groups with professionals (such as teachers, specialists who work with vulnerable children and youth social workers); 15 in-school workshops with a total of 232 children aged 8 to 17 from across the UK; 15 in-depth interviews with children identified as having had direct experience of online violent content.

Source 10: Ofcom Ipsos children's passive measurement pilot study 2023

Ofcom commissioned Ipsos to carry out a pilot study that passively measured the internet use of 162 children aged 8-12 across smartphones, tablets, and computers. The purpose of the study was to test whether passive methodology can in the future deliver robust metrics of children's online use.

Methodology

Devices were measured where the child's parent/guardian informed us during recruitment that the child used the device at least once a week.

A passive monitoring app/ VPN tracker was installed on the devices used by the child, which collected the data. The monitoring app could only be downloaded to iOS or Android devices; Amazon Fire tablets for children were not compatible with the app.

227 devices were measured: 127 smartphones, 79 tablets and 21 laptop/desktop.

We are aware that children share devices with other household members; as part of the recruitment process, parent/guardians of the children taking part informed us which devices that were to be tracked were shared with others. Family user mode was available on the tracking app for Android computers only which meant the device user could indicate who they were before their online activity was undertaken on the device, limiting irrelevant data collection on these devices.

---

[46] The research will be published on the Ofcom website on 13 March 2024.

A data cleaning process was implemented to ensure the data reasonably reflected the child's online behaviour and removed behaviour which was more likely to come from an adult. We initially began with 169 child participants but following the data cleaning process 7 participants were removed as the majority of their data reflected adult use leaving us with 162 participants. In some instances where participants had more than one device measured, devices which predominantly reflected adult use were removed. Overall (including the participants that were completely removed) 14 devices were removed.

The pilot study had fieldwork conducted during two phases. The first phase was a soft launch among 17 children whose online use was measured over a three-week period in January-February 2023. This small sample of children was used to ensure that the methodology of the research was appropriate. After confirming that the data collection from the first phase was successful, we continued the research with a larger sample. The second phase measured 145 children for four weeks during April-July 2023. Exact dates varied by participant, but all fieldwork fell 12 January - 26 February (phase 1) and 11 April - 18 July (phase 2). The results from both phases were combined to provide the unweighted data presented in this report. The data should therefore not be considered as robust.

Limitations

The study was conducted among a small sample of 162 8–12-year-olds and so only reflects the online use of the children in the study and may not be representative of all UK children aged 8-12.

One of the limitations with shared devices is that sometimes children share devices with siblings, that could have a similar behaviour or similar interests to them. For cases like this, we were unable to identify where the data came from the child participating on the study or their siblings, this is likely to remain an ongoing challenge for any future children's passive research.

A2. Category 1 research summary

Research requirements

A2.1 In accordance with our obligations under the Act for category 1, we have carried out research into:

- how easily, quickly and widely regulated user-generated content is disseminated by regulated user-to-user services;
- the number of users and the functionalities of the user-to-user part of such services; and
- other characteristics or factors relating to the user-to-user part of such services that Ofcom consider to be relevant to category 1 threshold conditions.

Summary of research findings

How easily, quickly and widely regulated user-generated content is disseminated by means of regulated user-to-user services.

Literature review

A2.2 We carried out a literature review into content dissemination on user-to-user services. The focus of our literature review was on factors that affect how 'easily, quickly and widely' content is disseminated. We found minimal existing research studying these precise criteria on online services. Some studies attempt to understand what factors affect how particular types of content spread across an online service. However, these studies generally focus on one type of harmful content only and often assess only one online service.

A2.3 There are various concepts used in the academic literature to assess the nature of content dissemination on online services. None of these are directly equivalent to 'how quickly, easily and widely' content is disseminated. 'Virality' is one concept used in academic work to assess how content is disseminated, though the exact meaning differs across studies. A similar concept that academics have used to measure the movement of content across an online service is 'structural virality', which combines measures of 'depth', 'size' and 'breadth' of content networks as constituent criteria. Finally, one study uses the term 'content half-life' as a measure of the speed of viewing or engagement with content. This concept measures the average time it takes for an item of content to receive half of its lifetime's engagement, i.e. if a piece of content received 100 views then this would be when 50 people had viewed the piece of content.[47]

A2.4 The literature suggests it is difficult to measure how quickly and widely content is shared, or the 'exposure' it receives in a quantifiable way or comparably across services. This is in part due to the lack of data accessible from the services themselves, which only rarely

---

[47] Graffius, S. M., 2023. Lifespan (Half-Life) of Social Media Posts: Update for 2023. [accessed 12 February 2024]

includes information about how many people have viewed pieces of content and at what time. [48]

A2.5　The literature review indicated that the size of the user base and service design (including functionalities) may play a role in content dissemination, but currently there is no consensus about the significance of separate elements, nor how they interact with one another.

A2.6　A focus of the literature is the role of content recommender systems as a primarily vehicle for services to increase users' time spent on the service and/or their engagement with content on the service. One study suggests that users spend less time on a social media service and engage less with the content on it when the content is curated by a purely chronological feed rather than an algorithmic feed. Algorithmic content recommender systems are designed to serve users with content that they find relevant and engaging and this study suggests that increases the time they spend on the service. This means that services may have an incentive to use content recommender systems because of the positive effect they have on user time spent and, potentially, long-term user retention. [49]

Assessment of the role of functionalities and other characteristics in the dissemination of content quickly, easily and widely

A2.7　The literature review indicated that certain functionalities or characteristics may play a role in how easily, quickly and widely content is disseminated. To supplement our understanding of the role that functionalities play, we carried out a logic-based assessment to identify the functionalities that enable quick, easy, and wide content dissemination.

A2.8　As there is no single source that lists all potential functionalities that an online service might provide, our understanding of functionalities was based on existing Ofcom analysis of the range of functionalities found on online services. The longlist of functionalities that we assessed was compiled from functionalities explicitly referred to in the Act as well as functionalities that were identified in Ofcom's Risk Assessment work (see Sources 3, 4). This existing work covers 69 functionalities that are known by Ofcom to be commonly found on user-to-user services. We also considered the role of content recommender systems as part of this exercise, reflecting the approach taken in Ofcom's risk assessment (see Source 5). References to functionalities in this Annex are to be construed accordingly. We note that the functionalities above may not be mutually exhaustive.

A2.9　In our exercise to examine relevant functionalities, we took the following into consideration. Taken together these functionalities can be considered as a proxy for virality:

　　a)　**Breadth**. In considering how widely content could be disseminated, we assessed: functionalities that increase or are intended to increase the potential range; and number of users that an item of content can reach.

---

[48] Global Network on Extremism and Technology (Lokmanoglu, A. D., Allaham, M., Abhari, R. M., Mortenson, C. and Villa-Turek, E.), 2023., *A Picture is Worth a Thousand (S)words: Classification and Diffusion of Memes on a Partisan Media Platform,* [accessed 12 February 2024].)

[49] Andrew M. Guess et al., *How do social media feed algorithms affect attitudes and behavior in an election campaign?,* Science, 381, 398-404 (2023).

b) **Ease**. We assessed the extent to which functionalities facilitated the uploading, generating, or sharing of user-generated content by users, irrespective of the speed or breadth with which the content may subsequently be encountered.

c) **Speed**. In considering how quickly content may be disseminated, we assessed: functionalities that reduce or are intended to reduce the duration of time between the uploading or generating of a piece of content and the point at which it may be encountered by users of the service.

A2.10 Each of the functionalities in our longlist were labelled as either relevant or not relevant to each of the three criteria in the research question: breadth, ease, and speed. For a functionality to be deemed of high relevance to the research question for category 1, it had to meet all three criteria: relevant to the quick *and* easy *and* wide dissemination of content. We used our judgement to assess which functionalities were the most relevant to these multiple criteria. We identified six functionalities and one characteristic that met these criteria:

- In-livestream chat
- Livestreaming one-to-many
- Livestreaming many-to-many
- Generate or upload content without an account
- Forwarding or re-sharing user-generated content with other users of the service
- Forwarding or re-sharing user-generated content onto other internet services
- Content recommender system

Full definitions of these features can be found in Annex A5.

A2.11 These six functionalities and content recommender systems each allow content to be shared quickly: they facilitate the instantaneous or near instantaneous sharing of user generated content among users of a service. They also allow the easy dissemination of user-generated-content through a lack of barriers to the uploading, generating, or re-sharing of content.

A2.12 The functionalities and characteristics all allow content to be shared widely; including with all of the participants of a livestream for the three livestream functionalities. 'Forwarding or re-sharing user-generated content within the service' and 'content recommender system' both allow for content to be shared to a wider audience than when it was first uploaded or generated. The 'generate or upload user-generated content without an account' functionality means that a service does not limit the potential contributors of content to a service, which in turn provides a wider potential creator base and audience for content.

A2.13 The logic exercise identified many functionalities that do not enable the quick, easy, and wide dissemination of content on services and that were subsequently excluded from further analysis. This included functionalities that enable users to access services (e.g. ways to create an account) and functionalities specifically enabling one-to-one communication.

A2.14 Additionally, some functionalities allow users to disseminate content quickly and easily, but only to a single or limited number of other users. Furthermore, even if the user base of a service is large, the service may include functionalities that limit the potential breadth of content distribution to a much smaller number of users. Our research found that the breadth of content dissemination on a service can be affected by other factors as well. This includes the overall user numbers of a service (discussed below) and the policies that a service provider uses to set a limit on the potential audience of a piece of content or

communication channel. These can be limitations that relate to the type of account a user holds. For example, a service may set policies that limit the number of pieces of content an account can upload, generate or share, sometimes based on how recently they joined the service. Service providers can also set policies that limit the activity of users regardless of the type of account they hold. This can include policies that impose numeric or defined limits to content dissemination or users' engagement activities with content such as forwarding or re-sharing. Finally, some service providers may impose policies that restrict or limit the time for which users can conduct certain activities. Examples include restricted time periods for engaging with other users on dating apps, maximum broadcast lengths on livestreaming services or ephemeral messaging time limits. There is often minimal public information available about these policies or service design factors and they often change over time. They can also differ across different parts of user-to-user services.

The functionalities of services

A2.15 We used Ofcom's database of service functionalities present on online services (**Dataset 2**) to analyse combinations of the six functionalities and one characteristic (content recommender systems) identified as playing an important role in the quick, easy and wide dissemination of content on user-to-user services.

A2.16 Dataset 2 shows that these functionalities and characteristics are common among services with a reach of 5% or greater in the UK's online aged 15+ population. The three of these functionalities/characteristics most commonly provided by services are:

- Forwarding or re-sharing user-generated content onto other internet services (61 of 101)
- Content recommender systems (44 of 101)
- Forwarding or re-sharing user-generated content with other users of the service (31 of 101)

A2.17 The types of service that most commonly provide at least one of the relevant functionalities/characteristics are:

- Information-sharing (20)
- Social media (14)
- Retail (12)
- Marketplaces and listing services (8)
- File-sharing (8)

A2.18 Thirty-seven services provide one of the six relevant functionalities and a content recommender system in combination. The types of service in Dataset 2 that provide at least one of the six relevant functionalities and a content recommender system are:

- Social media (11 services)
- Information-sharing (6 services)
- Pornographic services (5 services)
- Marketplaces and listing services (5 services)
- Video-sharing (4 services)
- Retail (2 services)
- Audio streaming (1 services)
- Gaming (1 services)
- Private communications (1 services)
- File-sharing (1 services)

A2.19   **Dataset 2** also shows us the most common combinations of the relevant functionalities and characteristics, which are the following:

- 26 services out of 101 had the functionalities 'forwarding or re-sharing user-generated content within the service' and 'forwarding or re-sharing user-generated content onto other internet services.'
- 31 services out of 101 had the functionality 'forwarding or re-sharing user-generated content onto other internet services" and had a 'content recommender system.'

A2.20   The combination of two functionalities that was the least observed among these services was 'upload or generate content without an account' and 'forwarding or re-sharing user generated content with other users of the service' identified together on none of 101 services.

The number of users of services

A2.21   **Dataset 1** includes 101 user-to-user online services assessed as likely in scope of the Act and with 5% or more UK aged 15+ online reach in October 2023 according to Ipsos iris. This list of 101 likely in scope user-to-user services formed the basis of the research team's analysis user numbers for category 1.
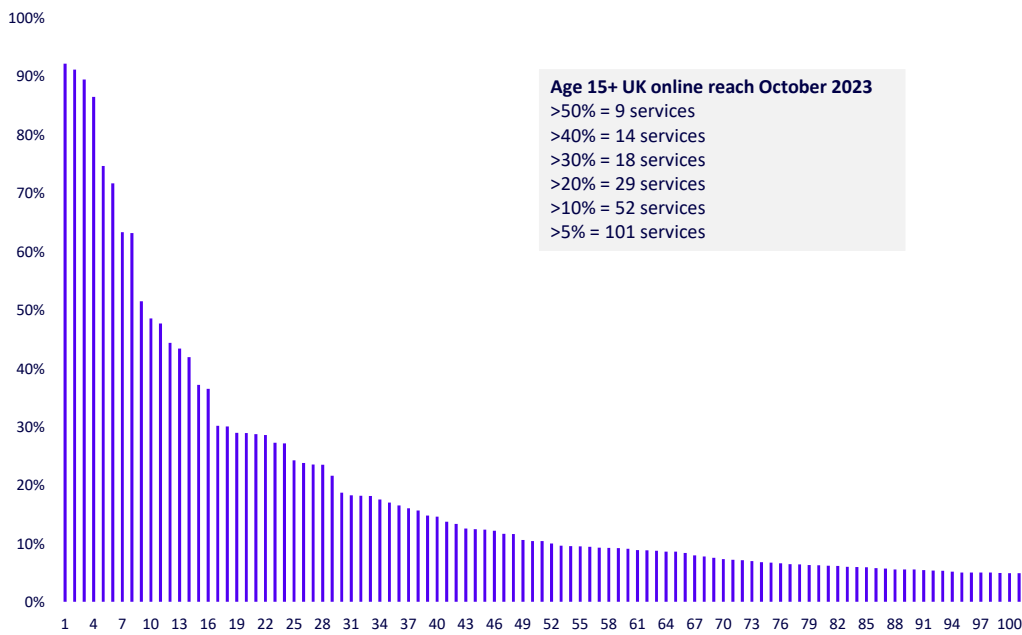
A2.22   Of the 101 services, 49 have an online reach of under 10%. There are only four services with a reach above 80%.

Figure A2.1: Cumulative number of relevant user-to-user online services that meet UK online aged 15+ reach threshold bands

UK online adult reach	>= 95%	>= 90%	>= 80%	>= 70%	>= 60%	>= 50%	>= 40%	>= 30%	>= 20%
Number of services	0	2	4	6	8	9	14	18	29

Source: Ofcom indicative assessment of in-scope services using Ipsos iris, Ipsos iris, Online Audience Measurement Service, October 2023, age: 15+, UK.

Figure A2.2: Ranked online aged 15+ UK reach of 101 user-to-user services identified as likely within scope: October 2023

Age 15+ UK online reach October 2023
>50% = 9 services
>40% = 14 services
>30% = 18 services
>20% = 29 services
>10% = 52 services
>5% = 101 services

Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services. Note: the reach figure for one service included here is from an Ofcom commissioned YouGov poll and not Ipsos iris, due to iris data for that service being partially reported. The self-reported data point from the YouGov poll had a reach of approximately 19% among UK internet users aged 16+.

A3. Category 2A research summary

Research requirements

A3.1   In accordance with our obligations under the Act for category 2A, we have carried out research into the following aspects of the search engine of regulated search services and combined services:

- the prevalence of search content that is illegal content and search content that is harmful to children;
- the number of users of the search engine; and
- other characteristics or factors that Ofcom consider to be relevant to category 2A threshold conditions.

Summary of research findings

The prevalence of search content that is illegal content and search content that is harmful to children

A3.2   There is very limited research available about the prevalence of harmful content on search engines. There is no established consensus on how to define or measure 'prevalence' in relation to harmful content on search engines. Prevalence is difficult to calculate on general or downstream search engines as search engines can index an enormous amount of the web's content, and it is challenging to assess content at that scale to determine the proportional presence of specific types of content. Sampling methodologies can provide some indicative insights on overall prevalence. Some studies of this nature have been carried out by Ofcom and the relevant findings are summarised below.

A3.3   Prevalence does not account for the prominence of harmful content, but ranking systems on search engines affect the likelihood of users engaging with different pieces of content. For these reasons, we conducted research about the prevalence, the prominence and the accessibility of illegal or harmful to children content as measurements for assessing the risk of harmful content being disseminated on search engines.

A3.4   Evidence from Ofcom's risk assessment for illegal content (Source 5) is summarised here:

- Ofcom's risk assessment found that search services have been used to access content that would amount to a range of offences, including terrorism, hateful content, extreme pornography, promotion of suicide and self-harm and child sexual abuse material (CSAM).
- The risk assessment also found evidence that the ranking process that search services use to prioritise content for users can be manipulated to increase the likelihood of illegal content being displayed near the top of ranked results. This includes the use of data voids by foreign state actors running foreign interference campaigns. This tactic of 'keyword stuffing' (filling a web page with keywords or numbers in an attempt to manipulate rankings of search results) or maximising data voids has also been observed in Ofcom research on fraud.

- The risk assessment also found that current evidence indicates that vertical search services pose less risk in relation to the relevant types of illegal content as they draw from a considerably narrower and defined set of sources for search results.

A3.5 Ofcom also conducted or commissioned four research projects in 2023 that studied the existence and prominence of content on search services that is both illegal and harmful to children. These studies cannot assess overall prevalence of illegal or harmful content on search services but do provide indicators of the potential risk through the assessment of samples of available search results. These studies analysed the presence, availability and prominence of content associated with the commission of fraud; the sale of illegal prohibited items including drugs, psychoactive substances, firearms and other weapons; foreign interference; and self-injurious behaviour (suicide, self-harm and eating disorders). Each study included an assessment of content available on between 2 and 5 search engines used by UK users in 2023.

A3.6 These research studies and relevant key findings are summarised in Annex A1. The key insights from the research studies for the purposes of categorisation research are listed here:

- **Prevalence of illegal or harmful content**: The four studies found that potentially illegal content and content harmful to children can be found on search services, including content for use in the commission of fraud and the sale of illegal weapons, drugs and psychoactive substances. Potentially illegal content was accessible on all the different search services studied, with no significant variations in the volume or prominence of this illegal content across the different search services that were tested in the studies. The largest sample study assessed the availability of content relating to self-injurious behaviour: in this analysis, across all search services tested, over 1 in 5 results contained content which may be harmful to children out of over 37,000 search results analysed.
- **Search features and risk**: The research suggested a range of search engine features that might affect the accessibility and prominence of potentially illegal or harmful content, but these differed for each type of illegal or harmful content studied. For articles used in the commission of fraud, these features included sponsored results/ads, autocomplete functions and 'related searches' functions. In research on the sale of prohibited goods on search engines, features that were shown to affect the prominence and accessibility of likely prohibited items included autocomplete, the type of media provided by the search product (i.e. text, image, video, shopping), and related and sponsored searches.

Role of other characteristics in the prevalence of search content that is illegal or harmful to children

A3.7 Using evidence from our risk assessment and research on harmful content, we considered what characteristics may be relevant to risk of harm and explored three in further depth:

a) Service type
b) Features
c) Business model

Service type

A3.8 Ofcom's work to date has identified different types of search services based on the definitions in the Act and how search services tend to operate in the current market.

- General search services enable users to search the contents of the web by inputting search queries on any topic and returning results. There are two types of general search service:

  ii) General search services which rely solely on their own indexing: These work by using crawlers (also called bots) to find content across the web ('crawling'); building an index of URLs by validating and storing the content found in a database ('indexing'); and using algorithms to rank the content based on relevance to the search query ('ranking').

  iii) Downstream general search services: As a type of general search service, downstream general search services provide access to content from across the web, but they are distinct in that they obtain (or supplement) their search results from those general search services which rely solely on their own indexing.

- Vertical search services: Also known as 'speciality search engines', these enable users to search for specific topics, or products or services offered by third party providers. They operate differently from general search services. Rather than crawling the web and indexing webpages, they present users with results only from selected websites with which they have a contract, and an API or equivalent technical means is used to return the relevant content to users. Common vertical search services include price comparison sites and job listing sites.

A3.9　Ofcom identified no available research into the risk of illegal offences or harm to children on vertical search engines. Ofcom's risk assessment (Source 5) argues that vertical search services present a lower level of risk of harm because these search services typically only provide access to a subject-specific, curated index of addresses. The risk assessment suggests that general search services (including downstream) can be used effectively to access illegal content, as discussed above.

A3.10　The existing literature indicates that search engines that are general or downstream may have a higher prevalence of content that is illegal or harmful to children. This is because the indexes of these services draw from a considerably greater pool of information.

Features of search services

A3.11　We examined key features relating to search services and considered the role they may play in the prevalence of content that is illegal or harmful to children.

A3.12　**Generative AI**: The evidence base concerning risks relating to the use of GenAI functions embedded in search engines is limited and not yet mature enough to rely on. However, there is some evidence to suggest that GenAI technologies on search services are at risk of amplifying the risk of harm to individuals. The extent to which GenAI is currently being deployed by search services is changing rapidly and is often hard to assess from publicly available information. One academic study demonstrates that Generative AI can be used or exploited by fraud actors. For example, it is possible for fraud actors to hide prompts in a website which can influence the behaviour of a chat-bot currently integrated in a popular search engine if the chat-bot is directed by the user to read that page.[50]

---

[50] Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T. and Fritz, M., 2023. Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. [accessed 12 February 2024]

A3.13 **Search query inputs**: There are several services that specialise in being able to search in certain forms of content, such a text-specialised services and image-specialised services. There is some limited evidence that suggests using images as a query can be an effective way for users to find services that sell drugs via search engines.[51] Ofcom research on prohibited goods highlighted that text search queries could be used to return potentially illegal search results, and in those selected cases text results returned the greatest proportion of potentially prohibited content (compared with image, video and shopping searches). As the evidence base is limited and inconclusive on the comparative risk associated with different search inputs, this is unlikely to be useful in advising on setting threshold criteria at this stage.

A3.14 **Search prediction and search personalisation (including auto-complete)**: Features that make suggestions related to a user's search requests can help users be more targeted or accurate in their searches. This is a common feature available on general search services. Ofcom's research confirms that these features can also help users to find a range of illegal content. For example, suggested searches and autocomplete functions were found to guide users to fraud-related content such as stolen credit card details.

A3.15 While we note that there is some limited evidence which may suggest these features can play a role in the prevalence of search content that is illegal or harmful to children, we consider that the evidence base is not sufficient to be used to draw robust conclusions.

Business model

A3.16 There is limited evidence on the links between different revenue models and the presence of illegal content in search results.

A3.17 Advertising-based models are common in the search market. For general search services that rely solely on their own indexing, advertising and sponsored results are the main pricing structures among the services. This is also the case for downstream general search services, but there are a handful of these services that adopt a subscription-based model.

A3.18 Evidence assessed as part of Ofcom risk assessment (Source 5) suggests that advertisements on search services may be misused for illegal activity. For instance, advertisements on search services can suggest products and sites to users that may enable them to engage in illegal behaviours or be exposed to illegal activity.[52] However, there is only limited research available that studies the link between advertising and potential harm via search engines. More research would be required to understand any link between advertising and the presence of content that is harmful to children or illegal.

A3.19 There is a wider diversity of revenue models among vertical search engines than general search services. Desk research found advertising and sponsored adverts/content and subscription revenue models in the vertical search service market. A common revenue model within this sub-market is commission-based revenue, with services receiving fees from third-party websites if users buy their product after being referred to them via the search service. There is no available robust evidence to assess the relationship between these varied business models and the risk of harm from search services.

[51] RAND, 2022. Commission On Combating Synthetic Opioid Trafficking – Technical Appendixes [accessed 12 February 2024].

[52] Ofcom, Online content for use in the commission of fraud - accessibility via search services, 18 September 2023, [accessed 22 February 2024], Ofcom, Sale of prohibited items on search services, 18 September 2024, [accessed 22 February 2024]

The number of users of services

A3.20 We used Ipsos Iris data from October 2023 to analyse the UK internet users aged 15+ reach of search services. We identified these as search services through internal indicative assessments of scope, with reference to the exemptions outlined in the Act (see Dataset 3).

A3.21 Two search services have markedly higher numbers of UK aged 15+ online visitors than all others in the measurable market. The top two services are search engines that create and use their own search indexes (general search engines) and have 85%, and 43% online visitor reach respectively.[53] The next largest search engine (a vertical search engine) has just 16% reach.

Figure A3.1: Ranked UK visitor reach of likely in-scope search services in the UK online 15+ population by search service type: October 2023
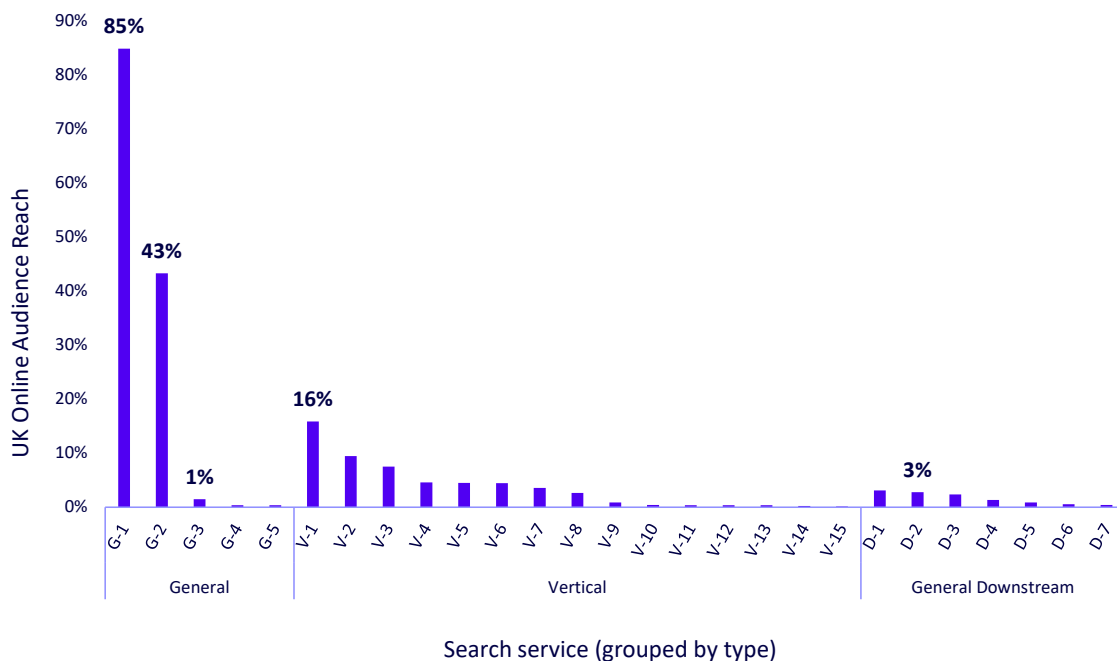
Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

---

[53] © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK

A4. Category 2B research summary

Research requirements

A4.1   In accordance with our obligations under the Act for category 2B, we have carried out research into:

- the dissemination of illegal content and content that is harmful to children by regulated user-to-user services;
- the number of users and the functionalities of the user-to-user part of such services; and
- other characteristics that Ofcom consider to be relevant to the category 2B threshold conditions.

Summary of research findings

The dissemination of illegal content and content that is harmful to children by regulated user-to-user services

Dissemination of illegal content

A4.2   Our analysis is based on Ofcom's Risk Profiles (Source 6), which summarises the key risk factors associated with illegal harm online. The evidence linking these functionalities to the manifestation of illegal harms online is summarised in Ofcom's risk assessment for illegal offences, 'The causes and impacts of online harm' (Source 5).[54]

A4.3   We identified functionalities[55] that are both particular to user-to-user services and relevant to content dissemination. To identify the functionalities which may be linked to an increased risk of illegal content, we ranked them by the number of illegal harms for which they were identified as key risk factors, and selected those that play a role in the dissemination of content.

A4.4   We focused on those functionalities that play a direct role in content dissemination. We construe these as functionalities that, in broad terms, allow users to upload, generate or share content on a service. This may include features that allow users to engage with content, content recommender systems, direct messaging, encrypted messaging, ephemeral messaging, group messaging, hyperlinking, live audio, livestreaming (including

---

[54] Ofcom's risk assessment considered priority offences and priority illegal content, which include terrorism offences, offences related to CSEA and other priority offences. These are detailed in Online Safety Illegal Harms Consultation Annex 5: Service Risk Assessment Guidance. So-called 'inchoate offences' are also treated as priority offences. To make the assessment as accessible as possible, Ofcom grouped the priority offences into kinds of illegal harms, such as 'Terrorism' and 'Proceeds of Crime' for example. Although included within Ofcom's risk assessment, the Risk Profiles did not take into account relevant non-priority offences, including communication offences.

[55] We also considered the role of content recommender systems as part of this exercise, reflecting the approach taken in populating the overarching functionalities list detailed in Annex 5. References to functionalities in this Annex are to be construed accordingly.

one-to-one, one-to-many), uploading or generating content (including text, videos and images), selling goods or services, sharing location information and video calling.

A4.5   We adopted this approach as it enables an evidence-based assessment of how functionalities affect the risk of illegal harms while still accounting for the wide variety of harms covered by the Act. It provides a means of prioritising the functionalities that might create risk for more types of illegal harm. We acknowledge that there are many possible ways to measure the risk of harm through the dissemination of illegal content and that this approach does not, for example, consider the differing severity of those harms or their divergent impacts on users.

A4.6   We identified three functionalities through this exercise:

   a) Direct messaging
   b) Encrypted messaging
   c) Uploading or generating content (images or videos)[56]

A4.7   Each of these functionalities is identified by the risk profiles as a key risk factor for seven types of priority illegal harms. They are each linked to a different combination of illegal harms, including child sexual exploitation and abuse, fraud, hate, intimate image abuse and terrorism.

A4.8   Direct messaging, sometimes referred to as private messaging, is typically construed as a user-to-user service feature that allows a user to send user-generated content directly to, or receive such content directly from, another user on a private channel.[57] Ofcom's risk profiles identify direct messaging as a risk factor for a number of illegal harms manifesting online, and as a *key* risk factor for seven types of illegal harms. The evidence that underpins Ofcom's risk profiles is summarised in Ofcom's risk assessment for illegal offences, 'The causes and impacts of online harm' (Source 5). This underlying evidence base provides more detailed analysis of the specific role that direct messaging plays in the dissemination of illegal content. Key findings relating to the risk of direct messaging are summarised below. It should be noted that authors of research referenced in Ofcom's risk assessment (Source 5) may use varying definitions of direct messaging but all are deemed sufficiently relevant for this context.

   • The ability to communicate on a regular basis is key to perpetrators establishing a grooming relationship with children away from public view and parental supervision.[58]
   • Perpetrators can share CSAM with one another via direct messaging. Interpol found that there was an increase in the volume of CSAM circulating via private messaging services or 'message applications' during the Covid-19 pandemic in 2020, which were centred around direct messaging.[59]

---

[56] The draft risk assessment refers to this functionality as 'post content (images or videos)'

[57] For these purposes we construe 'private channel' to be a part of the service where other users are unable to encounter the content sent or received (at least, without the sender or receiver taking subsequent action in relation to the content by means of the service).

[58] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.75.; See case studies analysed in source: Kloess, J. A., Hamilton-Giachritsis, C. E. and Beech, A. R., 2019. Offence Processes of online sexual grooming and abuse of children via internet communication platforms, *Sexual Abuse*, 31(1), pp.73-96.; Wolak, J., Finkelhor, D., and Mitchell, K. J., Ybarra, M. L., 2008. Online 'Predators' and their victims, *American Psychologist*, 63(2), pp.111-128.

[59] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.58.; Interpol, 2020. Threats and trends child sexual exploitation and abuse: COVID-19 impact. [accessed 12 February 2024].

- Direct messaging enables perpetrators to harass, stalk and threaten individuals in a targeted manner. The Suzy Lamplugh Trust found that texts or direct messages were the most common digital stalking behaviour.[60]
- Similarly, this type of targeted conduct could be hateful if the messages are racially or religiously aggravated. Ofcom research found evidence of direct messaging being used by perpetrators to target a victim with racist abuse.[61]
- Perpetrators of controlling or coercive behaviour are often able to send direct messages across multiple devices and services, allowing them to have a constant presence in the lives of their targets. This is an important tactic in controlling or coercive contexts.[62] In a UK-based Refuge study, an individual reported how a perpetrator contacted her 'professional and personal accounts with messages, hundreds of messages.'[63]
- Direct messaging is a key functionality that enables the non-consensual sharing of intimate images. The Revenge Porn Helpline found that non-consensual images were being shared via private messaging services; this was the method used in 18% of the cases where images were shared in 2020.[64]
- Direct messaging can be an enabler of fraud. Ofcom research found that, according to survey respondents, just under half (46%) of fraudsters use a targeted message to make initial contact with their victim, and typically this is done through direct messaging (41%).[65]

A4.9   Encrypted messaging, a form of messaging, both direct and group, that allows users to send and receive messages that are encrypted, is found to be a key risk factor for seven types of illegal harm. Key findings from Ofcom's risk assessment (Source 5) include the following:

- Direct messaging can allow terrorists to share content in a low-friction way with large numbers of like-minded people and encrypted messaging is particularly attractive to terrorist actors as it can reduce the chance of detection.[66]
- In terms of grooming, the introduction of end-to-end encryption makes it hard to detect offenders' contact with children and law enforcement agencies have highlighted the impact that increased prevalence of end-to-end encryption could have on detecting offenders and child safety.[67]

---

[60] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.113.; Suzy Lamplugh Trust, 2021. Unmasking stalking: a changing landscape. [accessed 12 February 2024].
[61] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.129.; Ofcom, 2023, Qualitative research into the impact of online hate. [accessed 12 February 2024].
[62] Problematic use of direct messaging requires an understanding of context for it to be identified as CCB. Repeated direct messages, like frequently messaging one's partner to check their location, can be harmless or abusive, depending on the overall context of the relationship. Source: Dragiewicz, M., Harris, M., Woodlock, D., Salter, M., Easton, H., Lynch, A., Campbell, H., Leach, J., Milne, L. 2019., Domestic Violence and communication technology: victim experiences of intrusion, surveillance and identity theft. [accessed 12 February 2024].; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.145.
[63] Refuge, 2021. Unsocial Spaces. [accessed 12 February 2024].
[64] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.213.; Revenge Porn Helpline (Ward, Z.), 2021. Intimate image abuse, an evolving landscape. [accessed 12 February 2024].
[65] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.240.; Ofcom, 2023. Online Scams and Fraud Research. [accessed 12 February 2024].
[66] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.32.
[67] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.58.; Virtual Global Taskforce, 2023. Statement on End-to-End Encryption.

- Encrypted messaging makes the exchange of CSAM hard to detect. Because of the difficulty in detecting CSAM over encrypted messaging, perpetrators are likely to seek out spaces with encrypted messaging to disguise their activity. [68]
- While potential perpetrators have been shown to use direct messaging for the sale of drugs and psychoactive substances, direct messaging that offers end-to-end encryption poses particularly risks due to the added security from detection that it offers. Analysis from the Center for Advanced Defense Studies demonstrated that suppliers of synthetic drugs use private Facebook groups to establish buyers' trust and often suggest continuing purchase conversations on private messaging services which provide end-to-end encryption.[69]
- Perpetrators seeking to sexually exploit others may use encrypted messaging to entice, manipulate, entrap and exploit victims and survivors into sexual activities for their own profit, with added security and privacy offered by encryption. A UN report found that the use of multiple services by traffickers shows that they are aware of the risk of monitoring or surveillance, so they often move their communication from open groups on social media services to encrypted or anonymised services such as a private messaging service.[70]
- Encrypted messaging services are inherently attractive environments for fraudsters, both as a location to commit or discuss fraud, as well as a destination to migrate potential victims who have been initially approached in non-encrypted online spaces. For example, romance scammers have been known to move conversations from dating sites to messaging services with end-to-end encryption.[71]
- Encrypted messaging can be used in the creation and amplification of disinformation content as part of foreign influence operations. Disinformation actors have used anonymous online spaces to create rumours and place fabricated content, spreading from these encrypted spaces to closed and semi-closed networks, to conspiracy communities, then mainstream social media, to finally end up being reported on in the mainstream media. Encrypted applications also lack the conventional fact-checking and content moderation that is offered on other services, thereby offering a unique opportunity to those wishing to easily spread disinformation.[72]

A4.10 The ability to upload content to, or generate text, images or videos directly on, the service is a very common feature of user-to-user services. It allows users to upload or generate content on open channels of communication. This functionality, in terms of video and image uploading, has also been identified as a key risk factor for seven types of illegal

---

[68] The exact scale of sharing and distribution of CSAM over encrypted messaging is difficult to quantify, as it cannot be tracked across services. Services offering end-to-end encryption have no means of accessing encrypted content. As such, technologies intended to mitigate the harm (such as hashing technology and content classifiers) cannot be applied within encrypted spaces and illegal content cannot be detected.; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.75.

[69] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.157.; C4ADS, 2020. Lethal exchange: synthetic drug networks in the digital era. [accessed 12 February 2024].

[70] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.185.; United Nations Office on Drugs and Crime, 2022. Global Report for Trafficking in Persons. [accessed 25 September 2023].

[71] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p241.;

[72] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p257.; Wardle, C., 2018: 5 Lessons for Reporting in an Age of Disinformation, *First Draft News*, 27 December. [accessed 12 February 2024]. Gurksy, J., Riedl, M. J. and Woolley, S., 2021. The Disinformation Threat to Diaspora Communities in Encrypted Chat Apps, *Brookings Institute*, 19 March. [accessed 12 February 2024].

harm. Key findings about this risk factor from Ofcom's risk assessment include the following:

- Services where content can be uploaded or shared on an open channel of communication can be conducive to the spread of terrorism content. For example, an article describes how, on the 20th anniversary of the September 11 attacks, a coalition of alt-jihadist meme producers ran a competition to see who could create the best meme of the attacks.[73]
- The ability to upload or generate content, in this case text, videos and images, is a key enabler of the commission of CSAM offences. Abusers can upload or generate visual CSAM (images and videos), and links or URLs to CSAM, on both open and closed channels of communication. For example, 77% of the CSAM reports dealt with by the Internet Watch Foundation in 2022 were from services which hosted images.[74]
- In terms of the promotion of suicide and self-harm, the ability to upload or generate content enables users to communicate and establish contact with others who are experiencing similar thoughts or behaviours, but the evidence shows that it is also being used to negatively influence users' thinking around suicide. A UK-based qualitative study[75] found that among self-harm patients, almost all had viewed others' posts on online services about self-harm methods, and had used these as a source of information that they could search to gain insight into experiences with these methods, or to decide on details of implementation.[76]
- In the context of coercive or controlling behaviour, uploading or generating content can be used to upload and share identifying information ('doxing'),[77] negative information, intimate images, and threatening words or images. Refuge report that 18% of victims and survivors had experienced doxing.[78]

---

[73] Alt-jihadists draw on the narratives of the alt-right and far right in Western culture wars while staying on brand with support for staple extremist groups such as Hezbollah, the Houthis, Hamas, the Taliban, Hayat Tahrir al-Sham, al-Qaeda, and the Islamic State." Ayad, M., 2021. An 'Alt-Jihad' is Rising on Social Media, *Wired*, 8 December. [accessed 12 February 2024]; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.32.

[74] "These sites provide 'storage' for images which either appear on dedicated websites or are shared within forums". Source: Internet Watch Foundation, 2023. The Annual Report 2022 #Behind the Screens: A deep dive into the digital and social emergency happening #BehindTheScreens, in children's bedrooms. [accessed 12 February 2024].; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.76.

[75] where participants had either previously used the internet for suicide-related purposes or had been admitted to hospital following serious self-harm)

[76] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.95.; Biddle, L., Derges, J., Goldsmith, C., Donovan, J L. and Gunnell, D., 2018. Using the internet for suicide-related purposes: Contrasting findings from young people in the community and self-harm patients admitted to hospital, p.12, *PLoS ONE*, 13 (5).

[77] The ability to upload or generate content, combined with user networks, facilitates 'doxing.' This describes sharing identifying information about a particular individual online with intent to cause harm or distress. Doxing often causes harm by encouraging other users in their network to join in with the harassment of victims and survivors.

[78] The Refuge study also provides qualitative examples of doxing in the context of domestic abuse. For example, 'Paula', whose former partner waged a campaign of harassment, publicly accused her of lying about the domestic abuse that she faced and encouraging others to abuse her. Direct threats of harm were made, and her name and address were publicly shared from the abuser's account. Source: Refuge. 2022. Marked as Unsafe. [accessed 12 February 2024].; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.145.

- The ability to upload or generate content, in particular images and emojis, is an important functionality in the supply of drugs and psychoactive substances online, as it can be used to promote drugs and signpost potential buyers. Volteface found that it was "common for dealers to post their drug 'menus' and price lists in their stories". This would include what drugs were available that day, with quantities and prices, and sometimes phone numbers so that customers could get in direct contact with the dealer.[79]
- The ability to upload or generate content, in this case images and videos, is an important functionality in the commission or facilitation of the extreme pornography offence. In 2020, Pornhub, an online pornography service, removed 10 million videos, amounting to about 80% of its content, after high-profile coverage raising concerns about the availability of illegal material, including CSAM and non-consensually shared intimate images, hosted on the service. There is a risk that services which attract adult content, particularly where illegal content has already been found, may also be the types of services where extreme pornography is found.[80]
- Uploading or generating content enables perpetrators of intimate image abuse to share content, and in some cases intimate images, in an open channel of communication for numerous users to see. Perpetrators have also been known to gain unauthorised access to victims' and survivors' accounts and to upload or generate intimate images from there.[81]

A4.11   While the functionalities listed above were identified as a key risk factors for the largest number of illegal harms, we note that other functionalities play a direct role in the dissemination of content and were also identified as key risk factors for illegal harms, albeit fewer types of illegal harms. For example, group messaging is a key risk factor for several types of illegal harms, including CSAM and Fraud, and forwarding or re-sharing content is a key risk factor for several illegal harms include the Foreign Interference Offence and Harassment, Stalking and Threats.

Dissemination of content that is harmful to children

A4.12   As to content that is harmful to children, we will be consulting on our register of risks relating to the causes and impacts of content that is harmful to children in spring 2024. Our preliminary findings are that the following functionalities are a risk factor when it comes to encountering content that is harmful to children – direct messaging, the ability to upload and generate content (in particular, images and videos), and content recommender systems. Our findings are not yet final.

---

[79] Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.158-159.; Volteface, 2019. DM for details: Selling drugs in the age of social media. [accessed 12 February 2024].

[80] Concerns were not necessarily raised about extreme pornography material, but primarily child sexual exploitation and abuse material and intimate image abuse (IIA). This is not a specific observation about potentially illegal and extreme content currently available on Pornhub. However, Pornhub's actions help us draw an inference that extreme pornographic content may exist on User-to-user services.; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.198.

[81] In one case, provided by the Law Commission, a woman's ex-partner set up a fake Facebook account in her name and uploaded intimate images of her, which were then viewed and copied to adult services. On one website the picture was viewed over 48,000 times. Source: Law Commission, 2021. Intimate Image Abuse: A consultation paper. [accessed 12 February 2024]; Ofcom risk assessment for illegal offences, 'The causes and impacts of online harm', p.214.

A4.13   Ofcom will soon publish research it commissioned on content on user-to-user services that is harmful to children.[82] The studies look at content promoting eating disorders, self-harm and suicide content, cyberbullying (which is facilitated by the dissemination and sharing of content) and violent content. [83] The studies and the relevant main findings are summarised below.

Key attributes and experiences of cyberbullying among children and young people in the UK
This research set out to explores, the key attributes and experiences of cyberbullying among children through focus groups and interviews with children and interviews with practitioners and school staff. Children, school staff and practitioners reported that cyberbullying happened anywhere young people interacted online and tended to concentrate on whichever platforms were most popular. Some participants suggested that cyberbullying behaviour differed between platform types, for example, negative comments around people's appearance were considered more likely to on image-based social media, in contrast to gaming platforms where the focus was often on gameplay. Functionalities involved in the direct dissemination of content were found to facilitate cyberbullying. Direct messaging, group chats and comment functionalities were identified as avenues in which users sent cyberbullying content. The ability to share/re-share original posts meant people were able to share content from or about someone to other sites and users without the original poster knowing. Children reported that it was easy to create accounts on most online platforms, often without identity verification. Children also reported that on some platforms, multiple accounts could be created by a single user, which could enable the creation of alias or fake accounts from which cyberbullying could take place with limited consequences.

---

[82] The research will be published on the Ofcom website on 13 March 2024.
[83] For cyberbullying in some cases the nature of the content itself may not be harmful, but the way it is being accessed and forwarded on the service can be. Cyberbullying can include a wide range of content, activity and behaviours. Examples relating to the dissemination of content can include uploading/generating/sharing content about an individual (including images, videos) or sharing content, jokes, negative comments, rumours, and /or sharing information or content they had previously shared with an individual/group; and directly targeting somebody, including uploading comments, trolling on a range of platforms, threatening and verbal abuse on gaming platforms.

Experiences of children encountering online content promoting eating disorders, self-harm and suicide

This research set out to understand the different pathways used by children to encounter online content that they felt promoted, glamourised and romanticised suicide, self-harm and eating disorder content. Children and young people in our sample reported a strong familiarity with the content. It was common for them to have multiple or regular encounters with such content and characterised it as being prolific on social media. Their encounters were sometimes unintentional (through personalised recommendations) as well as purposeful encounters (through searching, hashtags).

Functionalities involved in the direct dissemination of content were found to be used to share this type of content. Harmful content was often shared among friends online and in online fan groups, through both private messaging services/groups and social media posts.

Understanding pathways to online violent content among children

This research set out to understand the pathways through which children encounter violent content online. It explores what violent content looks like online, the impact it has on children and perceptions of safety measures to prevent children from encountering harmful content.

Similar to the other studies, functionalities involved in the direct dissemination of content were found to play a role in how children are exposed to violent content. Children's encounters with violent content were often unintentional, such as through personalised recommendations via a content recommender system and content unexpectedly being shared in large group chats. Some children were seeking out violent content, such as searching for violent content within platforms, and seeking out purpose-built user accounts and group chats dedicated to sharing violent content. There was a culture of sharing violent content among children (such as through screenshotting and reposting/forwarding the content), creating a cycle by which other children were then more likely to encounter the content.

A4.14   These research projects suggest that functionalities which relate to the dissemination of content that is harmful to children overlap with those we are considering through our illegal content analysis. The research indicates two broad types of functionalities that present risks to children in these harm areas: one is functionalities that enable the broad sharing and promotion of content on open channels, including via recommender systems; the second is functionalities that enable the direct dissemination of content to specific users, including direct messaging or closed groups.
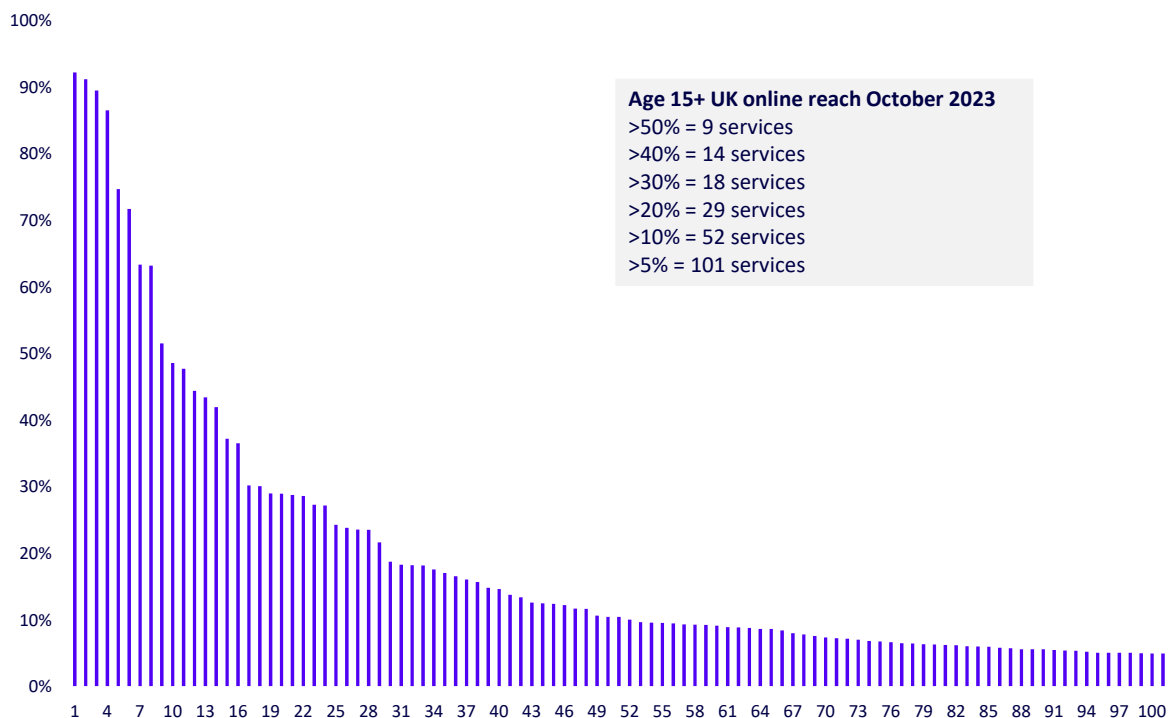
Functionalities on services

A4.15 The analysis above identifies functionalities that are associated with an increased risk of harm on services. The analysis below looks at the range of services that provide those specific functionalities or combinations of those functionalities.

A4.16 In common with our work to inform category 1 thresholds, our analysis of the presence of functionalities provided by user-to-user services is conducted using Database 2. The 22 functionalities included in Database 2 cover all the functionalities that are identified as key risk factors for illegal harms in the risk profiles (Source 6).

A4.17 Database 2 shows that the provision of relevant functionalities varies widely across the 101 user-to-user services. The most common functionality is the ability to upload or generate text, followed by the ability of users to upload or generate images. Searching for users/user generated content, uploading or generating text or multimedia content as a comment on existing user-generated content, forwarding or re-sharing user-generated content onto other internet services, and following/subscribing are each available on at least half of the services.

A4.18 As our research on harms indicates (see A4.2-A4.14), the risk of dissemination of illegal content and content which is harmful to children may be more common in situations where there is functionality that allows one user to communicate privately with another user. We therefore consider it instructive to analyse the presence of this functionality on relevant services.

A4.19 Functionalities related to the ability to communicate directly and privately with another user of the service are common, with direct messaging function provided by 67 of the services.

A4.20 The large majority of the 67 services that provide direct messaging functionality also allow users to also upload or generate text (59/67) and/or upload or generate images (53/67). Searching for users/user-generated content and forwarding or re-sharing user-generated content onto other internet services were also seen in 48 of the 67 and 43 of the 67 services, respectively. This demonstrates that many services that provide direct messaging often also allow users to upload, generate and share content through open channels.

The number of users of services

A4.21 Here we lay out our analysis of the audience of user-to-user services. As noted above, the practicalities and limitations of audience measurement systems mean that the user number data we can collect and analyse may differ from the definition of user in the Act. The audience measurement systems may not always be able to measure just the user-to-user part of a user-to-user service, and panel sizes may limit the ability to analyse user numbers by demographics.

A4.22 We use Dataset 1 to analyse the distribution of user reach across services deemed likely to be in scope of the regulations and with 5% or more UK aged 15+ online reach in October 2023, as measured by Ipsos iris.

A4.23 As seen in Figure A4.1, we identify a total of 29 services with a reach of 20% or more of the UK aged 15+ online population. This shape of this curve shows a long tail of services with lower reach, with 49 of the 101 services having a reach of under 10%.

A4.24 The comparative difference in user reach between each service decreases with the reduction in overall user base size.

Figure A4.1: Ranked UK online aged 15+ reach of 101 user-to-user services identified as likely within scope of the Act: October 2023

Age 15+ UK online reach October 2023
>50% = 9 services
>40% = 14 services
>30% = 18 services
>20% = 29 services
>10% = 52 services
>5% = 101 services

Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services. Note: the reach figure for one service included here is from an Ofcom commissioned YouGov poll and not Ipsos iris, due to iris data for that service being partially reported. The self-reported data point from the YouGov poll had a reach of approximately 19% among UK internet users aged 16+.

A4.25 In researching user numbers of the user-to-user services, we considered user numbers and reach among different demographic groups. Existing Ofcom analysis in Ofcom's Online Nation 2023 report suggests that while use of these services may differ from the population as a whole, for some demographic groups this did not generally change the shape of the reach curve.

A4.26 Recent Ofcom research has demonstrated that take-up of online services can vary among age groups.[84] Ipsos' children's passive measurement study (Source 10), as published in Ofcom's Online Nation 2023 report, indicates that many online services that have a large reach among UK adults are also widely used among children of ages 8 to 12.[85] Although it is not possible to make direct comparisons about the reach of individual services between our children's passive measurement panel and Ipsos iris data due to methodological differences, we do note that the top 6 highest-reaching social media brands among the online children aged 8-12 in our pilot research were also in the top 10 highest-reaching social media brands in May 2023, as measured by Ipsos iris.
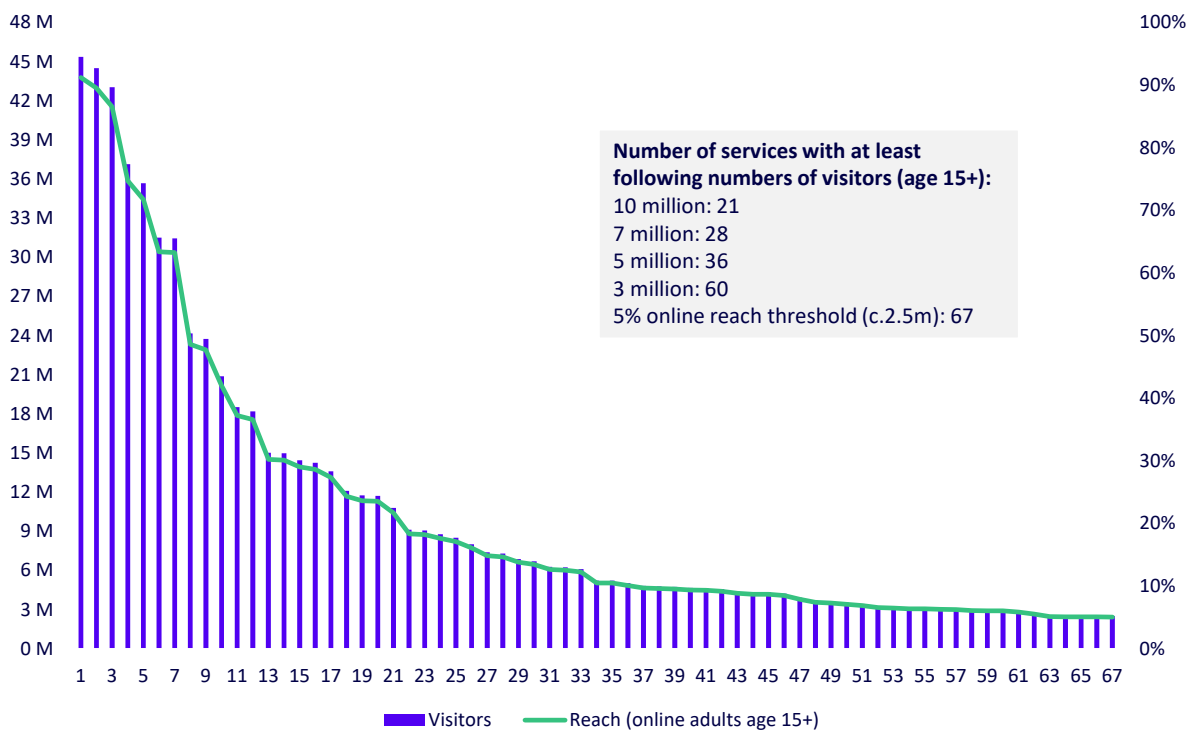
---

[84] Ofcom, 2023. Communications Market Report 2023: Interactive data.
[85] Ofcom, 2023. Online Nation: 2023 Report.

A4.27　Layering our analysis from Database 2 onto our user number database, we ranked the 67 services with direct messaging functionality by their UK aged 15+ visitor reach (Figure A4.2). The ranking of the 67 services produces a curve: 28 of these services have an audience of at least 7 million adults[86], while 60 of the 67 had an audience of at least 3 million adults.[87]

A4.28　It is important to note that online reach figures presented here are for individuals aged 15 and over who use the internet,[88] and that Ipsos iris does not measure internet use on some device types, meaning that 5% online reach in Ipsos iris equates to approximately 4% reach of the total UK population (i.e. approximately 2.5 million people). Likewise, given the gaps in audience measurement, the absolute audience numbers in the chart below will likely understate actual numbers of people accessing the service as those below age 15 are not being counted. This means that the number of services with total user numbers of three million or more may be greater than the 60 set out in our analysis below. Our explanation of how we have interpreted Ipsos iris reach data to understand the comparable UK-wide population user reach of services can be found in Annex A7.

Figure A4.2: Ranked UK online aged 15+ services identified within scope with 1-1 private messaging functionality: October 2023

Number of services with at least following numbers of visitors (age 15+):
10 million: 21
7 million: 28
5 million: 36
3 million: 60
5% online reach threshold (c.2.5m): 67

Source: © Ipsos, Ipsos iris Online Audience Measurement Service, 1-31 October 2023, age: 15+, UK, and Ofcom indicative assessment of in-scope services.

---

[86] I.e. 10% of the UK's total population of 67.0 million (6.7 million) to the nearest whole million
[87] I.e. 5% of the UK's total population of 67.0 million (3.35 million) to the nearest whole million
[88] A total of 50 million (to the nearest million) people aged 15 and over were internet users in October 2023 (Ipsos iris)

Other characteristics

A4.29   Ofcom's risk assessment for illegal harms (Source 5) assesses the evidence linking specific characteristics with the risk of illegal harms. These characteristics are functionalities, user base, business models, governance and other systems and processes. The risk assessment also incorporates assessment of the evidence linking certain service types to risk of harm.

A4.30   Based on that risk assessment, Ofcom's risk profiles (Source 6) identify three general risk factors that might affect the risk of harm on user-to-user services. These are user base demographics, business model and commercial profile. The profiles also identify seven service types as risk factors for a range of illegal harms.

A4.31   We have considered evidence relating to user base demographics as part of our analysis of the users of relevant services (see A4.28).

A4.32   Considering business model, the risk assessment finds that different business models (revenue models and growth strategies) may 'inadvertently increase' the risk of various illegal harms occurring on the service. However, there is little information available about the precise nature of many services' business models and services do not always fit neatly into a definition of one type of business model. Business models can evolve quickly over time and there is not a standardised and consistent way of labelling business models in the current market. The difficulty in classifying business models and the lack of evidence linking specific business models to the risk of specific illegal harms pose challenges to a potential use of business model as a threshold for categorisation.

A4.33   Considering commercial profile, the risk assessment finds that services operating at a variety of stages of commercial growth might experience increased risk of illegal harms occurring on their services. The evidence points specifically to early-stage services, low capacity services or services with a fast-growing user base. However, the evidence base in this area is thin, given the lack of publicly available information about the commercial profile of many individual services.

A4.34   Considering service types, the risk assessment identified links between seven service types and increased risk of a range of illegal harms. The type of content encountered on a service that advertises itself with a primary function as an adult service is likely to vary from the type of content encountered on a retail service or audio streaming service, even though there may be overlapping functionalities across all three service types. However, many user-to-user services provide more than one key purpose for users or serve more than one target audience. This means that the accurate and consistent labelling of user-to-user services within service types can be challenging and does not fit well with the requirement for clearly measurable threshold criteria for the purposes of categorisation.

A4.35   Overall, the challenges of definition and measurement for these characteristics, as well as the limited nature of the evidence base underpinning their links to risk of harm render these characteristics ineffective in establishing binary, measurable criteria for thresholds.

A5. Database 2: list of functionalities

Functionality	Definition	Relevant for category 1	Relevant for category 2B
Content recommender system	An algorithmic system that, by means of a machine learning model or other technique, determines or otherwise affects the way in which content (including user-generated content) is encountered by users of a service. Typically, content recommender systems are relied on by services to facilitate user engagement with content by means of the service.	Yes	Yes
Forwarding or re-sharing user-generated content with other users of the service	User-to-user service functionality that allows users to re-share content that has already been uploaded or generated by a user within the service.	Yes	Yes
Direct messaging	A feature that allows a user to send user-generated content directly to, or receive such content directly from another user on a closed channel of communication. A 'closed channel of communication' means a part of the service where other users are unable to encounter the content sent or received (without the user sender or receiver taking subsequent action by means of the service).	No	Yes
Forwarding or re-sharing user-generated content onto other internet services	User-to-user service functionality that allows users to re-share content that has already been uploaded or generated by a user onto other internet services.	Yes	Yes

Functionality	Definition	Relevant for category 1	Relevant for category 2B
Livestreaming one-to-one	User-to-user service functionality that allows users to simultaneously create and broadcast online streaming media in, or very close to, real time. This could also be described as a video call.	No	Yes
Livestreaming one-to-many	User-to-user service functionality that allows users to simultaneously create and broadcast online streaming media in, or very close to, real time.	Yes	Yes
Livestreaming many-to-many	User-to-user service functionality that allows users to simultaneously create and broadcast online streaming media in, or very close to, real time. This could also be described as a video-call.	Yes	Yes
Upload or generate text **Upload or generate images** **Upload or generate videos** **(3 functionalities)**	User-to-user service functionality allowing users to upload or generate content [text/image/video] on open channels of communication. *Note: Risk profiles refer to the ability to "post content", we have taken "upload or generate" to have the same meaning as "post" but decided to use "upload or generate" for Categorisation for the purposes of clarity.*	No	Yes
Upload or generate content without an account	User-to-user service functionality allowing users to upload or generate content [text/image/video] on open channels of communication without the need to be registered user of the service. *Note: Risk profile definition includes the ability to "post or send content anonymously".*	Yes	Yes

Functionality	Definition	Relevant for category 1	Relevant for category 2B
Upload or generate text or multimedia content as a comment on existing user-generated content	User-to-user service functionality that allows users to reply to content, or upload or generate content in response to another piece of content, visually accessible directly from the original content without navigating away from that content.	No	Yes
Encrypted messaging	User-to-user service functionality that allows users to send and receive messages that are end-to-end encrypted, i.e. cannot be seen by anyone other than the sender or the receiver.	No	Yes
Group messaging	User-to-user service functionality allowing users to send and receive messages through a closed channel of communication to more than one recipient at a time.	No	Yes
Live chat with a real person	User-to-user service functionality allowing users to exchange messages in real-time with another user, where the exchange can only take place if both users are online simultaneously. This does not include chat with AI assistants.	No	Yes
In-livestream chat	User-to-user service functionality allowing users to upload or generate text or other content alongside a live stream (see definition of livestreaming). The ability to upload or generate text or other content is removed once the live stream is ended.	Yes	No
Buying goods/services	User-to-user functionality allowing users to purchase goods and services from other users directly on the service,	No	Yes

Functionality	Definition	Relevant for category 1	Relevant for category 2B
Selling goods/services	User-to-user service functionality allowing users to upload or generate content dedicated to offering goods and services for sale. This does not include paid-for advertisements but may serve the function of allowing users to promote goods or service.	No	Yes
Speaking to others (oral, not one-to-one)	User-to-user service functionality that allows users to communicate with one another in real-time through speech or other sounds. *Note: Also known as live audio*	No	Yes
Create user groups	User-to-user service functionality allowing users to create online spaces that are often devoted to sharing content surrounding a particular topic. User groups are generally closed to the public and require an invitation or approval from existing members to gain access. However, in some cases they may be open to the public.	No	Yes
Follow/subscribe	User-to-user service functionality that allows users to follow or subscribe to other users. Users must sometimes be connected to view all or some of the content that each user shares. *Note: Also known as 'user connections'.*	No	Yes
Search for users/user-generated content	User-to-user service functionality that enables users to search for other users of a service, or for user-generated content.	No	Yes

A6. Measuring numbers of users

A6.1   In this section we set out the key principles we believe are required in relation to calculating the number of users of the user-to-user part of a user-to-user service, or the users of the search engine of a search service, for the purposes of producing the Register of Categorised Services.

A6.2   Our principles are guided by the fact that Ofcom must have regard to general duties under the Communications Act 2003, which include the need for regulatory activities to be transparent, accountable, proportionate, consistent and appropriately targeted. [89]

A6.3   Ultimately, our approach and process for measuring user numbers will be finalised after the Secretary of State makes the regulations specifying the categorisation conditions.

Essential requirements

A6.4   As a starting point, section 227(1) of the Act explains that a user is a "United Kingdom user" of a service if— (a) where the user is an individual, the individual is in the United Kingdom; (b) where the user is an entity, the entity is incorporated or formed under the law of any part of the United Kingdom.

A6.5   Our approach to measuring users must be compatible with the existing legal framework in the Act. The approach should also be able to be applied to a range of different types of services, including services which may have been operating for different periods of time or that have fluctuating numbers of users.

A6.6   Through responses to our Call for Evidence, we know that providers may take different approaches to measuring users on their service(s) and we are mindful of the need to ensure that providers are able to comply with their duties in a proportionate way. We consider a balance must be struck between ensuring that the user measurement methodology is prescriptive enough to ensure an acceptable level of certainty and consistency, while also being general enough to allow providers a degree of flexibility.

A6.7   We believe that our approach should be clear and transparent in order to give service providers certainty about how user number measurement should be interpreted. We considered whether providing guidance may be appropriate, but have concluded that the non-binding status of any such guidance (whether issued by the Secretary of State or Ofcom) could result in inconsistencies in measurement. This would likely cause confusion among industry stakeholders which may, in turn, undermine the integrity of the categorisation regime itself.

A6.8   For these reasons, we are of the view that the principles for determining how to count users of a service should be set in the Secretary of State's regulations relating to categorisation.

Other considerations

A6.9   We propose a single set of principles for both user-to-user services and search engines, to provide industry with a relatively straightforward framework that is easy for industry to

---

[89] Section 3 of the Communications Act 2003

understand and interpret. This should also ensure that combined services are not disproportionately affected by our proposals.

A6.10 Additionally, we have sought (where possible) to ensure that our approach accommodates existing industry practice. We have carefully considered responses to our Call for Evidence when developing these proposals.

Proposed approach

A6.11 We propose that thresholds that relate to user numbers refer to absolute numbers of users, rather than referring to 'reach' among the UK population.

A6.12 While our research measured users by reference to 'UK reach', we do not consider this to be an appropriate approach to a user number threshold. This is because the UK population will fluctuate – and therefore the number of users that represent a particular reach figure would also fluctuate, potentially resulting in uncertainty for industry.[90]

A6.13 In our view, the most appropriate way to count users for the purposes of the categorisation will ultimately depend on the service in question and the way in which it may be used by people or entities. We therefore think the right approach is to adopt a model that, so far as possible, is not prescriptive around the way in which users are to be counted for these purposes. This means a model that tracks the language of the Act to leave providers in no doubt as to its interpretation.

A6.14 The Act includes provisions and concepts that relate to users. The Act however does not stipulate a particular period of time for which services should measure their users (e.g. daily users, weekly users, monthly users). We consider it may be important for a time period to be specified, in order to provide certainty to providers and minimise inconsistencies in approaches taken by different services when reporting their user numbers.

A6.15 For the purposes of categorisation, we believe that the most appropriate approach is for service providers to report on **UK monthly users.** This proposal is supported by information we received in our Call for Evidence which indicated that measuring monthly users is a common approach. We also note that the EU's Digital Services Act also refers to monthly users.

A6.16 It is also necessary to set out the period over which a service should measure its monthly users. Without this, the user figures from providers may not reliably be compared with one another, which would undermine the integrity of the categorisation framework more generally.

A6.17 A service's user number figures may vary considerably from month to month, depending on numerous factors, some of which may be outside of their control. For instance, certain public events or highly popular news items could result in significant increases in in user traffic to a service.

A6.18 For this reason, we think that the **number of UK monthly users could be calculated as an average over a 6 or 12 month period**. In this proposal, we have sought to balance the need for the measurement period to be sufficiently long to ensure that the average number of

---

[90] Our approach to converting research on 'UK reach' to equivalent numbers of users in this advice is explained in A7 below.

UK monthly users is not overly affected by short-term fluctuations, while also ensuring that user trends and changes are reflected in the average in good time.

A6.19   There are scenarios where it is possible that a new service may already meet a set of threshold conditions when the service has been provided for less than the relevant measurement period. This may be more likely in cases where the service is made available by large or established providers. In this scenario we propose that the average be taken across the number of months that the service has been made available to users.

A7. How we have converted our research on visitor reach to 'number of user' measures for the population as a whole

A7.1 Throughout this document we have reported UK online 15+ visitor numbers and reach from Ipsos iris.[91] The measured population of this dataset is smaller than that of the total UK population, being limited both by age and whether individuals are counted as 'online'. According to Ipsos iris, in October 2023 there were 49,964,072 online individuals in the UK aged 15+, based on the latest PAMCo 2022-2023 survey estimates.

A7.2 For the purposes of recommending user number thresholds in this advice, we estimated population-wide figures that would be roughly equivalent to the reach figures used in the research.

A7.3 To do this, we mapped the online visitor data to equivalent total population reach figures, based on the most recent estimate of the total UK population at the time of publication.[92] These conversions have informed our recommendations for user number thresholds for all categories to ensure our recommendations are appropriate for the total size of the UK population, rather than the 15+ online population. The conversions are provided below.

Figure A7.1: Reach of UK population as a whole, mapped to equivalent Ipsos iris reach

UK population reach	5%	10%	20%	25%	30%	40%	50%
Absolute number of individuals (million)	3	7	13	17	20	27	34
Absolute number of individuals as equivalent Ipsos iris age 15+ reach	7%	13%	27%	34%	40%	54%	67%

Source: Ipsos iris, ONS, Ofcom calculations. Data in table presented to the nearest million/percentage point

Figure A7.2: Ipsos iris 15+ internet users to mapped reach of the UK population as a whole

Ipsos 15+ online reach	5%	10%	20%	25%	30%	40%	50%
Absolute number of individuals (million)	2	5	10	12	15	20	25
Absolute number of individuals as equivalent UK population reach	4%	7%	15%	19%	22%	30%	37%

Source: Ipsos iris, ONS, Ofcom calculations. Data in table presented to the nearest million/percentage point.

---

[91] A base of 49964072 internet users aged 15+ in October 2023
[92] ONS United Kingdom population mid-year estimate 2021 of 67026300 people
https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/timeseries/ukpop/pop

A8. Service type definitions

A8.1 The list below provides a brief explanation of terms used throughout this advice and is provided for convenience.

Service type	Definition
Social media services	User-to-user service type describing services that connect users and enable them to build communities around common interests or connections.
Payment services	User-to-user service type describing websites or applications that financial payment providers often have that enable users to send and receive money.
Information-sharing services	User-to-user service type describing services that are primarily focused on providing user-generated informational resources to other users
Marketplaces and listing services	User-to-user service type describing services that allow users to buy and sell their goods or services.
Video-sharing services	User-to-user service type describing services that allow users to upload and share videos with the public.
Gaming services	User-to-user service type describing services that allow users to interact within partially or fully simulated virtual environments.
File-sharing services	User-to-user service type describing services whose primary functionalities involve enabling users to store digital content and share access to that content through links.
Private communications	A user-to-user service type describing services that are typically centred around the sending and receiving of messages that can only be viewed or read by a specific recipient or group of people.
Audio streaming services	Service that allows users to stream audio e.g., music, podcasts, and audiobooks.
Retail services	Service that allows users to buy goods or services from the service itself.
Pornographic services	Services for pornographic content primarily provide or enable the dissemination of pornographic content (sometimes also described as 'adult content').