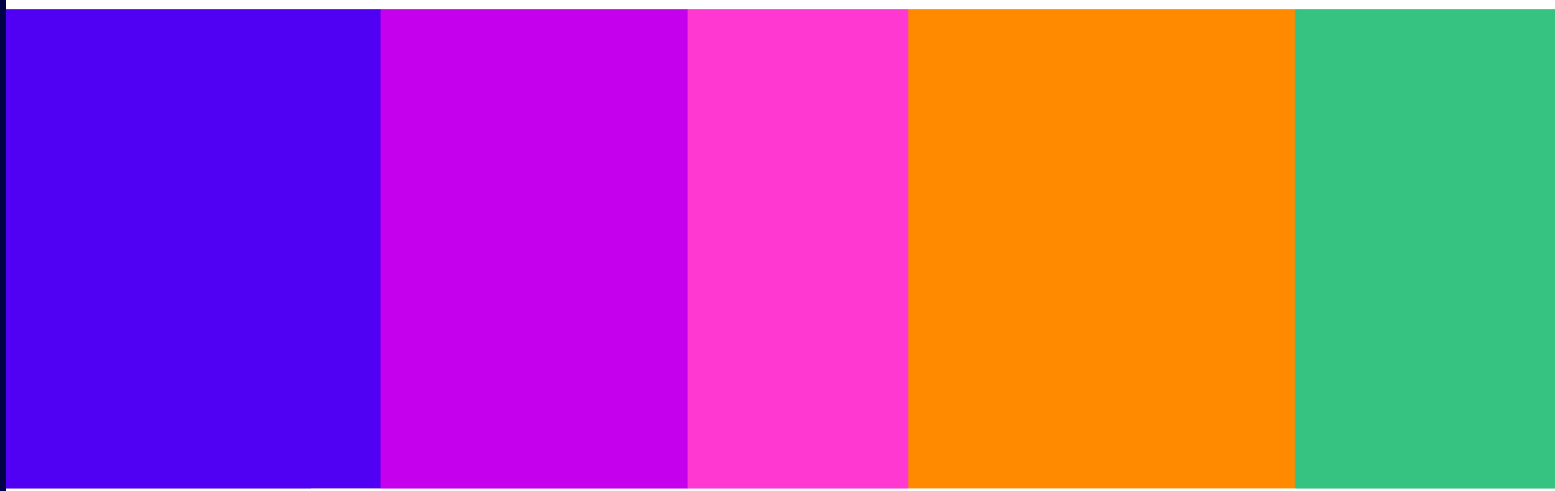


Protecting people from illegal harms online

Guidance on content communicated
'publicly' and 'privately' under the Online
Safety Act

Guidance

Published 16 December 2024



Contents

1. Guidance on content communicated ‘publicly’ and ‘privately’ under the Online Safety Act.....	3
About this document.....	3
Role and status of this guidance.....	3
Structure	4
Relevant statutory framework.....	4
General guidance	5
Guidance on each of the statutory factors.....	7
Case studies	11

1. Guidance on content communicated ‘publicly’ and ‘privately’ under the Online Safety Act

About this document

- 1.1 This document provides high-level guidance on the concepts of content communicated ‘publicly’ and ‘privately’ within the Online Safety Act 2023 (‘the Act’).
- 1.2 It is intended to assist providers of user-to-user (U2U) services looking to comply with their online safety duties by taking measures that relate specifically to content communicated ‘publicly’, as set out by Ofcom in a Code of Practice (‘Code’).
- 1.3 A provider taking such a measure must ensure that it is taken in relation to all content communicated ‘publicly’ by means of the service (subject to any further relevant provision in the measure). In the first instance, providers must assess for themselves (taking this guidance into account) the content that is communicated ‘publicly’. However, section 232 of the Act specifies a number of factors that Ofcom must consider when deciding whether content is communicated ‘publicly’ or ‘privately’. These should also be the starting point for providers. This document builds on those factors by providing high-level guidance on how we would expect to approach this when determining if a provider has properly applied measures recommended in a Code to content communicated ‘publicly’.
- 1.4 This guidance is intended to be relevant to services of all sizes and types. It is not intended to set out precisely where the boundaries between content communicated ‘publicly’ and ‘privately’ lie.¹

Role and status of this guidance

- 1.5 One of our regulatory principles is that we will regulate in a transparent manner. Guidance can serve as a useful means to achieving this principle and to increasing understanding of our approach to regulation.
- 1.6 Whether or not a provider has applied measures set out in a Code to content communicated ‘publicly’ will depend on the specific facts in each case. Providers should seek their own independent advice if they are unsure about this. We cannot, as a matter of law, limit our discretion as to any future decision. Accordingly, although this guidance sets out at a high level the approach we would normally expect to take, it does not have binding legal effect, and each case will be considered on its own merits.

¹ We note that some offences specified as priority offences in the Act also use concepts of ‘public’ and ‘private’, but this guidance is not relevant to interpreting those offences. See Ofcom’s Illegal Content Judgements Guidance in relation to those offences.

- 1.7 If we decide to depart from this guidance, we will set out our reasons for doing so. This guidance may also be subject to revision from time to time. This may be, for example, to reflect experience from our supervisory and enforcement work, or in light of technological developments.

Structure

- 1.8 This guidance is structured as follows:
- relevant statutory framework
 - general guidance about the concepts of content communicated ‘publicly’ and ‘privately’
 - guidance on each of the statutory factors
 - case studies

Relevant statutory framework

- 1.9 The Act provides Ofcom with the power, if it considers it appropriate, to include in a Code of Practice a measure describing the use of a kind of technology (paragraph 13(1) of Schedule 4). This includes the power to recommend a measure describing the use of ‘proactive technology’ as a way (or one of the ways) of complying with some of the duties set out in the Act.²
- 1.10 Proactive technology is defined in section 231 of the Act. Broadly speaking, this refers to: (1) ‘content identification technology’, except where this is used in response to a report from a user or other person about particular content; (2) ‘user profiling technology’ (which excludes technology deployed in the circumstances referred to in section 231(5) of the Act); and (3) ‘behaviour identification technology’, except where this is used in response to concerns identified by another person or an automated tool about a particular user.
- 1.11 The Act refers to measures describing the use of proactive technology as ‘proactive technology measures’.
- 1.12 There are constraints on our power to include proactive technology measures in a Code. Importantly, where the technology operates (or may operate) by analysing user-generated content (UGC) or metadata relating to such content, the measure may not recommend the use of the technology to analyse UGC communicated privately, or metadata relating to UGC communicated privately (paragraph 13(4) of Schedule 4).³
- 1.13 Section 232(2) of the Act specifies three factors (in particular) that Ofcom must consider when deciding whether content is communicated ‘publicly’ or ‘privately’ by means of a service. These are:
- the number of individuals in the United Kingdom who are able to access the content by means of the service

² Paragraph 13(3) of Schedule 4 to the Act provides that a proactive technology measure may be recommended only for the purpose of compliance with illegal content, children’s online safety or fraudulent advertising duties (specifically, those duties set out in sections 10(2), 10(3), 12(2), 12(3), 27(2), 27(3), 29(2), 29(3), 38(1) or 39(1)).

³ User-generated content is defined in section 55(3) of the Act.

- any restrictions on who may access the content by means of the service (for example, a requirement for approval or permission from a user or from the provider of the service)
 - the ease with which the content may be forwarded to or shared with (1) users of the service other than those who originally encounter it or (2) users of another internet service
- 1.14 As explained in paragraph 1.3, this document is intended to provide further practical guidance to providers of U2U services on the concepts of content communicated ‘publicly’ and ‘privately’ insofar as they are relevant to measures set out in any of our Codes.
- 1.15 For completeness, we note that any proactive technology measures included by us in a Code which recommend analysis of UGC or metadata relating to such content are limited to regulated UGC or metadata relating to regulated UGC. This excludes:
- a) emails
 - b) Short Message Service (SMS) messages
 - c) Multimedia Messaging Service (MMS) messages
 - d) one-to-one live aural communications
 - e) comments and reviews on provider content
 - f) identifying content that accompanies content within any of (a) to (e)
 - g) news publisher content⁴
- 1.16 Accordingly, irrespective of whether such content might be considered as communicated ‘publicly’ or ‘privately’, proactive technology measures do not recommend analysis of these specific types of UGC (or metadata related to such content).

General guidance

- 1.17 The question is whether the *communication* of the content is public or private, rather than whether the content itself is of a ‘private’ nature. As a result, whether content is communicated ‘publicly’ or ‘privately’ for the purposes of the Act will not necessarily align with whether that content engages users’ (or other individuals’) rights to privacy under Article 8 of the ECHR.^{5 6}
- 1.18 When determining whether a provider has applied measures to all content communicated ‘publicly’, we expect to take a pragmatic approach. In particular, we recognise that providers will need to make decisions about whether content is communicated ‘publicly’ at scale, and do not expect them to make judgements about this at the level of individual pieces of content present on their service. Instead, when considering if a provider has acted in accordance with a measure set in a Code, we expect our focus to be on the systems and processes operated for this purpose and their outcomes.

⁴ ‘News publisher content’ is defined in section 55(8) of the Act.

⁵ For example, it is possible that users might have a right to privacy under Article 8 of the ECHR in relation to content which is communicated ‘publicly’ for the purposes of the Act. Conversely, users may not have a right to privacy under Article 8 of the ECHR in relation to content which is nevertheless communicated ‘privately’ for the purposes of the Act.

⁶ Similarly, where providers are processing any personal data (whether or not that data is communicated ‘publicly’ or ‘privately’ for the purposes of the Act), providers should undertake such processing in compliance with relevant data protection legislation.

- 1.19 We expect providers to make their assessment based on the information reasonably available to them that is relevant to all three factors, and the inferences they may reasonably be expected to make in light of this.
- 1.20 Whether content is communicated ‘publicly’ or ‘privately’ will depend on the relevant factual context. This will be determined by taking account of each of the statutory factors and any other factors that we consider relevant.
- 1.21 We would expect providers to use a consistent approach in determining which content is communicated ‘publicly’ on their service. Maintaining a record of their assessment may help providers to achieve greater consistency.
- 1.22 Providers may identify one or more additional factors that they consider relevant to assessing whether content has been communicated ‘publicly’ on their service. We would expect providers in this case to record – and be able to justify – why they consider these to be relevant. Any decision on whether those factors are relevant (and, if so, how they should be taken into account by providers) will ultimately rest with Ofcom.
- 1.23 Factors that we would not expect to be relevant to the question of whether content has been communicated ‘publicly’ or ‘privately’ include:
- the fact that content has been generated, shared, or uploaded by a user that has anonymity or is using a pseudonym
 - the fact that content (or any parts of the service on which that content is generated, shared, or uploaded) is labelled as ‘private’
- 1.24 Providers should be mindful that the Act does not stipulate that any one statutory factor should carry greater weight than another, and all three statutory factors (and any other relevant factors) will need to be considered together.
- 1.25 Whether content has been communicated ‘publicly’ or ‘privately’ may change over time. For example, content may only have been accessible to a small user group when it was first uploaded and may have been communicated ‘privately’. If changes are made to the access restrictions meaning that a far larger number of users are able to access that content, it may subsequently become ‘publicly’ communicated content.⁷
- 1.26 The fact that content was originally communicated ‘privately’ when it was generated, uploaded, or shared to a service does not mean that any subsequent communications of that same content (for example, ‘reposts’ of that same content by other users) should also be considered as communicated ‘privately’.

⁷ For the purpose of applying any measures set out in a Code that recommend analysis of content communicated ‘publicly’ before or as soon as practicable after it can be encountered by users, we would expect content whose status changes from being communicated ‘privately’ to ‘publicly’ to be analysed before or as soon as practicable after it becomes content communicated ‘publicly’.

Guidance on each of the statutory factors

Number of UK individuals able to access the content (A)

- 1.27 As explained in paragraph 1.13, we are required by section 232(2)(a) of the Act to consider the number of individuals in the United Kingdom who are able to access the content by means of the service.
- 1.28 To identify how many users are able to access the content, any access restrictions on who may access the content by means of the service (under the second statutory factor) need to be taken into account. We discuss these separately in paragraph 1.33.
- 1.29 The greater the number of individuals in the UK who are able to access the content, the more likely it is to be communicated publicly. Importantly, content does not need to be accessible by *all* internet users to be considered as communicated ‘publicly’. Where it is accessible to a substantial section of the public, it should be considered as communicated ‘publicly’.⁸ We have included some case studies at paragraphs 1.48 to 1.62 to help providers understand how we would likely approach an assessment of the three statutory factors.
- 1.30 Providers should be mindful of the following points.
- This statutory factor refers to individuals in the United Kingdom. This is consistent with the scope of the safety duties regarding U2U services, which (where expressed to apply in relation to users of a service) extend only to the design, operation, and use of the service as it affects United Kingdom users of the service.⁹
 - This factor refers to the number of such individuals who are ‘able’ to access the content by means of the service, rather than the number of individuals that are accessing (or have accessed) the content. The fact that content has only been accessed by a small number of users in practice does not preclude it being considered as communicated ‘publicly’. Conversely, where there is evidence that a large number of users have accessed content (and therefore are demonstrably able to access it) this may be a highly relevant factor in deciding whether it has been communicated ‘publicly’, even if some access restrictions appear to be in place.
 - Even though content may be accessible to less than a substantial section of the public, that does not mean that it should automatically be considered as communicated ‘privately’. For example, if there are some access restrictions in place but it is very easy for users to share or forward that content, that content might be considered to be communicated ‘publicly’.
 - The fact that it may be difficult for individuals to access the content (for example, because users need time to locate the content or it is not easily discoverable) does not mean that content should be considered as communicated ‘privately’.
- 1.31 We recognise that there may be limitations in the provider’s knowledge about the number of individuals that are able to access content. For example, a user may choose to share their password to their account with other users without the service provider’s knowledge. As

⁸ This is the case irrespective of the second and third statutory factors (such as any access restrictions on that content, or the ease with which that content can be shared with or forwarded to other users of the service other than those who originally encounter it or users of another internet service).

⁹ See section 8(3) of the Act.

explained in paragraph 1.19, we expect providers to make their assessment of whether content has been communicated ‘publicly’ or ‘privately’ based on the information reasonably available to them.

Access restrictions (B)

- 1.32 We are required by section 232(2)(b) of the Act to consider any restrictions on who may access the content by means of the service. One example of an access restriction in the Act is a requirement for approval or permission from a user or from the provider of the service.
- 1.33 In general terms, it is relevant to consider any features that affect user access to the content, including any settings that are applied either by the user or the service provider. This could include, for example, whether there are default privacy settings in place to restrict access to the content, or whether the user has restricted the content’s availability to other users of the service (for example, whether the user has stopped other users seeing the content without their active permission).
- 1.34 Unless the provider has evidence to the contrary, we would expect the following to constitute access restrictions:
- a requirement for an individual to enter credentials (for example, a password or biometrics) before being able to access the specific content
 - a requirement for an individual to receive an invite or obtain permission from another user before being able to access the content
 - a requirement for users to have access to a decryption key to access the content, where that key is only available to specific individuals¹⁰
- 1.35 While a restriction on accessing content based on age verification or age estimation would amount to an access restriction that may result in a section of the public being unable to access the content, we would not expect this by itself to mean that such content is communicated ‘privately’. This is because, in the absence of any other restrictions, the content would remain accessible to a substantial section of the public.
- 1.36 There are also some important constraints on what can constitute access restrictions for the purposes of determining whether content has been communicated ‘publicly’ or ‘privately’. In particular, section 232(3) of the Act specifies that the following do not count as restrictions on access:
- a requirement to log in to or register with a service (or part of a service)
 - a requirement to make a payment or take out a subscription to access a service (or part of a service) or to access particular content
 - inability to access a service (or part of a service), or to access particular content except by using particular technology or a particular kind of device, as long as that technology or device is generally available to the public (this would include, for instance, a service accessible by an app installable only on a particular mobile operating system)
- 1.37 A subscription or registration requirement is different to a privacy setting (as described in case study 4). A privacy setting would limit who can access the specific content, whereas,

¹⁰ We note that user to user services should only apply measures where it is technically feasible for them to do so.

under a subscription model, any member of the public who pays the subscription fee would be able to access that content where there are no privacy settings in place.

1.38 Additionally, we do not expect the following to be considered ‘access restrictions’ for these purposes:

- a requirement for user identity verification before content can be accessed on a service
- the fact that there is no search functionality on a service, making it more difficult in practice for individuals to locate the content – what is relevant is whether it is discoverable or accessible by members of the public
- the fact that there are restrictions on who can interact with or respond to content (for example, by commenting on it)
- the fact that the technical design of the service means that it has only limited capacity to accommodate concurrent users (however, providers can, and may wish to, consider such thresholds when determining the number of UK users who are able to access the content under the first statutory factor).

1.39 If there are no access restrictions in place, then the content should be considered as accessible to all UK internet users for the purpose of the first statutory factor.

1.40 Providers should be mindful of the following points.

- The fact that there are access restrictions on a service does not necessarily, by itself, mean that content on that service is communicated ‘privately’.¹¹ We would still expect a service provider to consider how many individuals in the UK are able to access the content, and the ease with which it can be forwarded to or shared with users of the service other than those who originally encounter it (or with users of another internet service).
- The fact that content is accessible only to individuals that are part of the same community or organisation (for example, because they are employees of the same company) may amount to an access restriction.¹² However, this is not by itself sufficient to result in that content being considered communicated ‘privately’.
- Even if messages shared among a group are to be considered as communicated ‘privately’, other content associated with that group may be considered as communicated ‘publicly’ if the access restrictions do not extend to that content. For example, even if messages shared between a small number of users are considered as communicated ‘privately’, it is possible that the name and profile picture for that group should be considered as content communicated ‘publicly’ if they can be accessed by all users on that service.
- The effect of access restrictions may change over time. For example, if default privacy settings apply when content is first shared, but those settings are subsequently changed

¹¹ As explained in paragraph 1.29, where it is (notwithstanding any access restrictions) accessible to a substantial section of the public, content should be considered as communicated ‘publicly’.

¹² Providers should be mindful, as discussed in relation to sharing or forwarding of content, that the design of some access restrictions may encourage or facilitate the sharing or forwarding of content with users of the service other than those who originally encounter it, or with users of another internet service. For example, where a user can send an unlimited number of invites to individuals without any form of identifier associated with those individuals (such as an email address).

to allow the content to be more widely accessible, this could mean that content originally communicated privately is subsequently considered as communicated publicly, and vice versa.

Sharing or forwarding of content (C)

- 1.41 We are required by section 232(2)(c) of the Act to consider the ease with which the content may be forwarded to or shared with users of the service other than those who originally encounter it, or with users of another internet service.
- 1.42 We consider the focus of this factor to be on any features, functionalities, or settings included in a service that facilitate the forwarding to or sharing of content with individuals that do not already have access to that content. Examples might include:
- a functionality that facilitates the ‘reposting’ of content (either on the same or a different internet service)
 - a functionality that enables users to ‘tag’ in any other user of the service (or another service)
 - a functionality that enables those with access to a ‘closed’ user group to add further individuals to that user group and, in doing so, to provide them with access to historical content
- 1.43 We maintain that the focus should not be on the ease with which the content might be forwarded or shared *by the person* who uploaded or generated it. Instead, the focus should be on the ease with which it may be forwarded or shared *by the recipients* of that communication.
- 1.44 The easier it is for recipients to share or forward content with individuals other than those who originally encounter it (whether by means of the service or another internet service) using features, functionalities, or settings included in the service, the more likely it is to be considered as content communicated ‘publicly’.
- 1.45 Where a service includes functionality to share or forward content to others, any restrictions or ‘frictions’ incorporated within that functionality should be considered, as they may limit the ease with which the content may be shared or forwarded. For example:
- where content may only be shared with or forwarded to other users where the sharing user has prior identifying information (such as knowledge of their mobile number or email address)
 - where content may only be shared with or forwarded to a limited number of individuals at a time (for example, because of a quantitative forwarding limit)
 - where relevant restrictions on content access, in line with the second statutory factor, are in place (such as where the content can be shared from a closed group to an undefined audience, but where members must be individually invited and accepted by privileged group members, and where the content is thereafter encrypted with only specific users having access to a decryption key).
- 1.46 We recognise that it is possible for content to be shared or forwarded from any internet service (for example, by a user taking a screenshot of that content and then sending it to another user, or by a user who has been given a password to access specific content choosing to share that password with other individuals) and that it may be virtually impossible for services to use technical means to prevent online content from being shared

in this way. We do not expect this to indicate that content can be forwarded or shared with ease for the purpose of this third statutory factor.

1.47 Providers should be mindful of the following points.

- This factor requires a qualitative judgment to be made about the ease with which content may be subsequently shared or forwarded. The fact that content has not been forwarded or shared with users of the service other than those who originally encounter it (or users of another internet service) does not mean that that content may not be shared or forwarded in such a way with ease. Conversely, where there is evidence that content has been shared with a large number of users (and therefore it is demonstrably easy to share or forward it) this may be a highly relevant factor in deciding whether it has been communicated ‘publicly’.
- The fact that it is easy to share or forward content is not necessarily, and by itself, determinative that content has been communicated ‘publicly’. We would still expect providers to consider how many individuals in the UK are able to access the content and any restrictions on who may access the content by means of the service.
- Similarly, the fact that it is not easy to share or forward content is not by itself determinative that such content has been communicated ‘privately’. As noted in paragraph 1.29, where content is already accessible to all or a substantial section of the public, it should be considered as having been communicated ‘publicly’.
- Providers’ risk assessments will consider, among other things, how easily, quickly, and widely content may be disseminated by the service. Assessments will also consider the level of risk of service functionalities facilitating the presence or dissemination of content. We would expect service providers’ risk assessments and views on the ease with which content may be shared or forwarded (for the purposes of considering whether content should be considered as communicated ‘publicly’) to be consistent.

Case studies

1.48 This section sets out case studies which are intended to help providers understand how we would likely approach a holistic assessment of all three statutory factors.

Case Study 1

User A needs to create an account and be logged in if they wish to post their content or interact with other users’ content (for example, to reply to a post) on an online forum. However, there is no need to register with the service to read content that is posted on it. Only a small number of users access the forum on average per month.

1.49 Content that User A posts to the online forum is communicated ‘publicly’.

1.50 Even though users need to log in or register with the service to post their content or interact with other users’ content, this does not count as an access restriction under the Act. It does not matter that only a small number of users access the service in practice. The point is that there are no access restrictions in place and content posted to the service by User A is accessible to all internet users.

Case Study 2

User B has an account on a video-sharing service. They upload videos to share with a small number of other users who subscribe to or follow their account. To access the service (and content posted on it), users are required to take out a subscription and register by providing their personal details. User B has not applied any privacy settings to restrict access to their videos, nor has the service. However, except for users who subscribe to or follow their account, User B's content is not easily discoverable or searchable by other users because of the amount of content uploaded to the service.

- 1.51 User B's content is communicated 'publicly'.
- 1.52 The fact that only the small number of users who subscribe to or follow their account are likely to encounter (and access) their content, and that it would be difficult for other users of the service to locate or discover it, does not, by itself, mean that it should be considered as communicated 'privately'. Any registered user of the service can, in principle, access that content. In addition, although there is a requirement to register and take out a subscription to access the service, these do not amount to access restrictions under the Act and so we would consider the service (and videos shared on it) to have no access restrictions. As per our guidance, the content should therefore be considered as accessible to all users for the purposes of the first statutory factor.

Case Study 3

User C is in a channel with a small number of users on an online service where they share content with one another. The channel has settings in place which mean that other users must be invited to join, either by the channel administrator or another member of the channel, to access content shared within it. However, there is functionality within the service for User C and others with access to the channel to forward or share content they receive within the channel with their other contacts (even if those other contacts have not been invited to join that channel).

- 1.53 Content that User C shares within the channel is communicated 'privately'.
- 1.54 Only a small number of users are able to access the content. The requirement for a user to receive an invite to join the channel, and to therefore be able to access content within it, amounts to an access restriction (unless there is evidence reasonably available to the service provider which demonstrates that it is not). The fact that the content can be forwarded or shared by User C would not be relevant to the third statutory factor. While there is functionality for others with access to the channel to forward or share the content with others outside that channel, the ease of sharing or forwarding is limited as content can only be shared with or forwarded to other users where the sharing user has prior identifying information (such as their mobile phone number).

Case Study 4

The same scenario as Case Study 3 applies. However, one of the other users in the channel (User D) shares a piece of content that User C had shared by 'reposting' it to another part of the online service. This has no privacy settings applied to it, so anyone who is registered with (and logged into) the service can access content that User D, or any other user, has uploaded to that part of the service.

- 1.55 In this scenario, the content uploaded by User D is communicated 'publicly'.

- 1.56 Although in Case Study 3 content shared within the channel was communicated ‘privately’ by User C, this is a new communication of the content by User D. There are no access restrictions in place on this part of the service, so we would consider the content to be accessible to all internet users for the purposes of the first statutory factor. It is irrelevant how easily content posted by User D can be shared or forwarded as it would be communicated ‘publicly’ based on the first two statutory factors alone.

Case Study 5

User E is in a group chat with a very large number of other users on an online messaging service. Settings applied by the service provider mean that content shared within the group chat is only accessible by users who are members of the group chat, with access to a decryption key required to access the content.

- 1.57 Content shared by User E within the group chat is communicated ‘publicly’.
- 1.58 We would generally consider a requirement for users within the group chat to have a decryption key to access content to be an access restriction under the second statutory factor. However, the fact that there is an access restriction in this case study does not, by itself, mean that content shared by User E within the group chat should be considered communicated ‘privately’. The number of individuals in the UK who are able to access the content also needs to be taken into account. In this case, we would consider content shared within the group chat to be accessible by a substantial section of the public due to the large number of users being members of the group chat.¹³

Case Study 6

User F has an account with an online file storage and sharing service to which they upload their content. Access to User F’s content is password-protected and they have shared that password via functionality within the service with a small number of friends and family. Those users to whom User F has granted access can, via functionality within the service, share User F’s content – but only with other specific users – by entering known identifying information into the service (such as their email address).

- 1.59 User F’s content is communicated ‘privately’.
- 1.60 Only a small number of users are able to access User F’s content by means of the file-storage/sharing service. Unless there is evidence to the contrary, we would expect a requirement for an individual to enter credentials, like a password, and to receive an invite from User F to access the content, to constitute access restrictions. While there is functionality within the service for recipients of User F’s content to share it with other users, the ease with which this can be done is limited because any new user must be individually invited and known to the sharing user in some way to have their identifying information.

¹³ We recognise that providers of some end-to-end encrypted services may not have this level of information available to them. We expect providers to make their assessment based on the information *reasonably* available to them that is relevant to all three factors, and the inferences they may *reasonably* be expected to make in light of this.

Case Study 7

User G has an account with an online dating service and has been matched by the service with a stranger, User H. User G has been invited by the service to generate or upload a short video introducing themselves and share it with User H via a messaging part of the service (and vice versa). No other users on the service can access the video message, nor is there any functionality to forward or share it.

- 1.61 User G's video message is communicated 'privately'.
- 1.62 Only User H is able to access User G's content. User G has sent the video message directly to User H via the online dating service to view, and there is no functionality within the online dating service for User H to forward or share User G's video message with any other users either on the service or via another internet service.