Protecting people from illegal harms online

Volume 3: Transparency, trust and other guidance

Statement

Published 16 December 2024

Contents

Section

Annex

1. Introduction to the Volume

In this volume, we provide further **transparency** and guidance to providers to help them better protect users. We consider these decisions will help serve the objective of **building trust** in service providers and in the regulatory regime.

It sets out the decisions we have taken in producing the following three guidance documents:

- Our Illegal Content Judgements Guidance (ICJG) will help providers understand what illegal content is and what information they should have regard to when making judgements about content.
- Our enforcement guidance, which has been informed by our experience and track record in other sectors, sets out in clear terms how we will normally approach enforcement under the Online Safety Regime.
- In our guidance on content communicated 'publicly' and 'privately' under the Online Safety Act, we have set out the factors providers should consider when determining whether content is communicated 'publicly' and included some case studies case studies which we intend to assist stakeholders and provide greater clarity.

What are we trying to achieve

1.1 As set out previously in this statement, we expect implementation of the Online Safety Act 2023 (the Act) to ensure people in the UK are safer online by delivering four outcomes:

a) stronger safety governance in online services;
b) online services are designed and operated with safety in mind;
c) greater choice for users so they can have more meaningful control over their online experiences, and
d) greater transparency regarding the safety measures services use, and the action Ofcom is taking to improve them, to build trust.

1.2 There is an important wider context, that Ofcom's approach, both in all other parts of this statement, but also in how we set up and maintain the regulatory regime, needs to engender trust and that part of the mechanism of achieving that is through transparency.

1.3 Ofcom is accountable to Parliament and to the public, and we are committed to being fully transparent in our work as a regulator, and how we will enforce the regulatory regime. For example, our supervision work will engage some of the highest risk and reach services to help ensure they have the systems and processes in place to improve the safety of users, and our transparency work will shed light on both good and bad practices, encouraging the former.

1.4 We note that independent research has found that when regulated firms and other stakeholders share the purpose of regulation and see it as fair and effective, they are more likely to support its implementation and contribute to achieving its goals.1 In part,

[1] Hodges, C., 2022. 'An Introduction to Outcome Based Cooperative Regulation'. Outcome-Based Cooperation: In Communities, Business, Regulation, and Dispute Resolution. [accessed 2 October 2024].

achieving this trust is also a by-product of achieving the strategic objectives we discussed in the previous two volumes.

1.5 In this volume, we provide further transparency and guidance to services to help them better protect users. We consider these decisions will help serve the objective of building trust in service providers and in the regulatory regime.

What decisions have we made towards this objective

1.6 We consider the following regulatory documents (and associated rationales), will contribute to our strategic objectives in relation to transparency and trust:

a) The **Illegal Contents Judgement Guidance (ICJG)** sets out detailed guidance to services to help them determine whether content is likely to be 'illegal content' or not.[2] Publishing clear guidance on this will increase the chances that services remove illegal content and reduce the probability that they over moderate out of an abundance of caution. It will also increase transparency about what types of content users can be expected to be protected from. Chapter 2 explains our approach to the ICJG. The **ICJG** can be found here.

b) Our **Enforcement Guidance** details our decisions related to our approach to enforcement. The Act grants Ofcom a range of enforcement powers and requires us to publish guidance on how we will exercise them. Setting out clear guidance about when we exercise our enforcement powers will also help ensure that the operation of the regulatory framework is transparent and predictable for service providers. Chapter 3 explains the rationale behind our enforcement guidance. Our **Enforcement Guidance** can be found here.

c) Our **guidance on content communicated 'publicly' and 'privately'**, explains the approach we have taken in providing guidance about when service providers should consider content to be communicated 'publicly'. Service providers in scope of any proactive technology measures will need to ensure those measures apply to content on their service that is communicated 'publicly' (and not 'privately'). As part of that guidance, we have provided case studies to help services calibrate and make informed trade-offs between the different factors they need to consider.[3] We note that this guidance was not a requirement under the Act, but we consider it a necessary piece of additional guidance to provide more clarity to services. Chapter 4 explains the thinking informing our **guidance on content communicated 'publicly' and 'privately'**. Our public private guidance can be found here.

[2] As set out in Chapter 2 of this volume, services can choose to use this guidance, or alternatively use their own terms and conditions, as long as the latter is inclusive of all illegal content in the UK.

[3] Section 232 of the Act specifies factors which Ofcom must, in particular, consider when deciding whether content is communicated "publicly" or "privately" by means of a user-to-user service. The factors are: (a) the number of individuals in the United Kingdom who are able to access the content by means of the service; (b) 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 the provider, of the service); (c) the ease with which the content may be forwarded to or shared with (i) users of the service other than those who originally encounter it, or (ii) users of another internet service.

2. Ofcom's Illegal Content Judgements Guidance

What is this chapter about?

The Act requires us to provide guidance to service providers about how they can judge whether a piece of content is likely to be illegal and we do this in the Illegal Content Judgements Guidance (ICJG). In making such judgements, the approach to be followed is for service providers to consider whether there are 'reasonable grounds to infer' it is illegal content (that is, that it 'amounts to a relevant offence'), using all relevant information reasonably available to the provider ('reasonably available information') to make this judgement. Definitions of 'reasonable grounds to infer' and 'reasonably available information' are set out in the final guidance.

In this chapter, we set out a high-level summary of what the ICJG proposals for the November 2023 Consultation on Illegal Harms were, and the stakeholder responses we had to those proposals. We then set out the decisions we have made with regard to specific stakeholder responses. We have split this section into two; one focusing on cross-cutting or broader issues, and the other on more offence-specific issues. We have also included separate annexes setting out less substantive responses and changes, and further detail on our original proposals.

What decisions have we made?

We have considered stakeholder responses and made a number of offence-specific decisions which are set out in the following chapter. These include the following:

- **Fraud by false representation**: At consultation, we provided a list of indicators which, when present in specific combinations, would provide reasonable grounds to infer that content amounts to an offence of fraud by false representation. On review, we believe such an approach was too rigid as the indicator list could become quickly out-of-date. As such, we have decided to steer service providers to consider these indicators as illustrative and non-exhaustive. We have also altered the organisation of our list of indicators, basing the four groups of indicators on the four necessary requirements of the offence.
- **Intimate image abuse (IIA)**: At consultation, we proposed that, when content is shared, reposted or forwarded, the state of mind that matters is that of the user sharing, reposting or forwarding. We have decided to strengthen this position in relation to IIA. Absent any evidence that the user reposting, forwarding or resharing content has taken appropriate steps to ascertain consent, it is reasonable to infer that the user does not have a reasonable belief in consent. It follows that if the content concerned is an intimate image which has been shared without consent, it will be illegal content when it is forwarded, shared or reposted. This strengthening of our guidance will provide extra protection to victims and survivors of IIA.
- **Sexual exploitation of adults**: In light of evidence provided to us during the consultation process, we have given additional guidance on how service providers can recognise content related to the sexual exploitation of adults. The ICJG lists a series of risk factors which service providers should consider when assessing whether posts are likely to

amount to offences related to the sexual exploitation of adults. Where enough of these risk factors are present, we set out that, absent evidence to the contrary, these posts are illegal content .

- **Encouraging/assisting suicide and self-harm**: We have made numerous changes to these chapters, drawing out the nuance in relation to the language, the vulnerability of users posting potentially illegal content and instances where intent may be able to be inferred.
- **Cyberflashing**: At consultation, we proposed that it would not be possible to infer intent to cause distress, alarm or humiliation in most cases. We have now decided to amend our position and state that service providers can infer intent in most instances, except for in certain, very specific circumstances. This change of position will strengthen protections for victims of cyberflashing.

Alongside this, we have streamlined and refined the ICJG to make it more accessible and better reflective of the law. We have also set out the information we consider reasonably available for service providers in a box for each offence, and added new sections to each chapter to draw out more clearly what types of content may need to be considered for the purposes of risk assessment.

Why are we making these decisions?

We have made these decisions in order to better reflect the law, to make the ICJG is as accessible as possible, and to ensure that our approach is informed by evidence provided by stakeholders. We have at all times sought to strike an appropriate balance between user protection and user rights.

Introduction

2.1 This chapter outlines our decisions on the Illegal Content Judgements Guidance (**'the ICJG'**), following our November 2023 Illegal Harms Consultation and our August 2024 Further Consultation on Torture and Animal Cruelty.

2.1 Section 192 of the Online Safety Act (**'the Act'**) sets out the approach that providers of in-scope services have to take when they are required to make a judgement about whether content is illegal content or a particular kind of illegal content. In making such judgements, the approach to be followed is whether they have 'reasonable grounds to infer' it is illegal content (that is, that it 'amounts to a relevant offence'), using all relevant information reasonably available to the provider ('**reasonably available information**') to make this judgement. Definitions of 'reasonable grounds to infer' and 'reasonably available information' are set out in the final guidance in paragraphs 1.40 to 1.53 and 1.60 to 1.70 respectively.

2.2 Section 193 of the Act creates a duty for Ofcom to produce guidance on how providers can make illegal content judgements for the purposes of the takedown duty, the risk assessment duty and the safety duties more generally (the 'Illegal Content Judgements Guidance'). In addition, the ICJG will assist Category 1 services in relation to their duties relating to fraudulent advertising and news publisher content.[4]

[4] These are additional duties in relation to Category 1 services. In March 2024 we published our call for evidence regarding these additional duties. This has since closed, and we are working towards a consultation

2.3 The regulatory regime established by the Act is not a content regulation regime. That is, Ofcom does not regulate providers' treatment of individual items of content, nor will Ofcom take decisions on items of content. However, providers must assess the risk that users will encounter illegal content on their services and the level of risk of harm to them that such content presents. They must also take appropriate and proportionate measures to protect their users from illegal content.

2.4 As a part of the duties established by the Act, service providers must have proportionate systems and processes designed to take down illegal content of which they are aware, swiftly. Broadly speaking there are two ways services can meet this duty. They can make illegal content judgements applying the guidance set out in the ICJG. Alternatively, (in the exercise of their own right to freedom of expression, with which Ofcom has no powers to interfere), they can draft their own terms and conditions in such a way that, at a minimum, all content which would be illegal in the UK is prohibited on their service for UK users. They would then be able to make content moderation decisions based on their terms and conditions. In practice we think it likely that many services will take the second of these approaches, or a hybrid approach.

2.5 The ICJG is intended to help providers make illegal content judgements in general, for the purposes of their risk assessments and duties to protect users, and specifically, for the purposes of the takedown duty. It will also help providers check that their terms and conditions do protect their users from all illegal content.

2.6 More specifically, the ICJG is intended to:

a) Give an overview of priority and relevant non-priority offences as set out in legislation and common law, by setting out the three parts of each offence (conduct or actus reus, state of mind or mens rea, and defences) and how these offences have been interpreted in practice;
b) Set out the 'reasonably available information' that providers should take into account when making content judgements about each offence;
c) Explain how providers may use reasonably available information to make reasonable inferences about whether content 'amounts to' an offence', so that they can judge whether there are 'reasonable grounds to infer' that the content is illegal content;
d) Provide guidance about the state of mind or mens rea element of offences, where relevant.

2.7 Our final version of the ICJG has been written regarding our duties under section 3(4A) of the Communications Act 2003. It has also been written in compliance with our requirement to carry out our duties in a way that is compatible with the Human Rights Act 1998, including Article 8 and Article 10 of the European Convention on Human Rights ('ECHR').[5]

2.8 In this chapter, we first outline our primary proposals in relation to the draft ICJG and the responses we received to our consultation, and then set out our decisions in regard to the final version. The annex titled 'Annex 1 to the statement on Further stakeholder responses' provides further detail on some offence-specific responses and decisions.

---

setting out our proposals. If we need to amend this guidance we will consult on proposed amendments at the time.

[5] Article 10 protects your right to hold your own opinions and to express them freely without state interference. Article 8 protects your right to respect for your private life, your family life, your home and your correspondence.

Our proposals and stakeholder responses

2.9 In November 2023, we consulted on a draft form of the ICJG.

2.10 As part of our consultation, we made the following policy proposals.

a) In relation to reasonably available information, we proposed:

i) *Not* to require service providers with a larger size or capacity to consider additional or different reasonably available information to smaller providers;
ii) To take a 'technology-agnostic approach' which did not presuppose how information was retrieved or analysed;
iii) To highlight the risk of malicious reporting.

b) In relation to inferences about state of mind, we noted the following:

i) that state of mind is a necessary part of some offences and cannot be put aside, regardless of the difficulty of making inferences about it;
ii) that, where content has been forwarded, shared or reposted, the state of mind which should be considered in most instances is that of the user who forwarded, shared or reposted;
iii) that, as stated in the Act, where content has been posted by a bot, inferences about the conduct and the presence of the mental element, and any defences, should be made by considering: the actual person controlling the bot or tool, where this is known to the service; or the person who may be assumed to be controlling the bot, where the actual identity of the person is not known;

and proposed that:

iv) in some cases (that is, in offences related to possession of extreme pornography and 'making' of child sexual abuse material), an offence's state of mind requirement can be inferred to be met by posting of content in itself.[6]

c) We proposed to focus primarily on priority offences as set out in the Act, covering non-priority offences only where they were created by the Act.
d) Where we judged that content amounting to one offence would automatically amount to another (for example, because stalking involves harassment, any stalking content would automatically classify as harassment content), we proposed to steer providers to consider the simplest offence with the lowest bar, and therefore only gave guidance on this simpler offence.
e) In relation to defences we proposed that:

i) general defences are unlikely to be relevant to a service's illegal content judgements as it is difficult to imagine circumstances in which services would have reasonable grounds to infer that they arise, and so will not be outlined in the ICJG; and
ii) in cases where a relevant defence is that the user has a 'reasonable excuse' to believe something to be the case, we have considered what 'reasonable' might mean in an online context.

2.11 More information on our original proposals can be found in the annex titled 'Annex to Volume 3.'

[6] Bots are an umbrella term that refers to a software application or automated tool that has been programmed by a person to carry out a specific or predefined task without any human intervention. Bots are often employed on services to post content at scale without the need for repeated human intervention.

2.12 We made detailed proposals in relation to specific offence areas and offences, based on a review of statute and case law, as well as proposals on what information is reasonably available to providers. We invited technical corrections as well as more substantive challenges to our interpretation of the law, comments on the accessibility of the draft ICJG and comments on our view of reasonably available information.

2.13 We received numerous responses from stakeholders, some focusing on policy issues raised in specific offence chapters, and others commenting more broadly on our approach to the ICJG's primary concepts (such as 'reasonable grounds to infer' and 'reasonably available information') or on the accessibility of the ICJG. We have set these out in the section titled 'Cross-cutting.'

2.14 We are grateful for the detailed consideration that many stakeholders gave on difficult and sensitive areas of UK law. We have assessed all suggestions on a case-by-case basis and where we have accepted these without further comment or with minor amends, this is indicated in the annex titled 'Annex 1 to the statement on Further stakeholder responses'.

Cross-cutting

Accessibility and clarity

2.15 While some stakeholders, for example, **Google**, **Nexus** and **Stop Scams UK**, praised the thoroughness and clarity of the ICJG or deemed it sufficiently accessible, several responses (an individual stakeholder, **Yoti,** the **Advertising Standards Authority,** the **Canadian Centre for Child Protection (C3P))** argued that the length, complexity and legal nature of the ICJG makes it insufficiently accessible for service providers. In particular, small providers and those without access to advice and expertise shared a need to understand legal terminology (the **Federation of Small Businesses**).[7] One stakeholder suggested that an understanding of regulatory law and/or the legislative process is necessary to understand the ICJG.[8] **Protection Group International** said that the ICJG is not detailed enough or easy enough to navigate and called for a way to search or find relevant points in the style of a quick guide.[9] The **New Zealand Classification Office** called for a summary of and more accessible form of the ICJG to be made available to the public. [10]

2.16 We recognise that the issues covered in the Illegal Content Judgements Guidance can be legally and conceptually complex, and the language used to cover them is often dense and technical. In drafting each section, we have aimed to balance legal accuracy with accessibility, and to use a 'Plain English' approach where possible. We have provided extensive legal detail in an annex which gives an overview of relevant offences as they appear in legislation. This annex has allowed us to summarise offences in a more accessible way in the main chapters. However, while we have tried to prioritise readability, the use of

---

[7] Advertising Standards Authority response to November 2023 Illegal Harms Consultation, p. 10. Canadian Centre for Child Protection (C3P) response to November 2023 Illegal Harms Consultation, p. 34. Are, C response to November 2023 Illegal Harms Consultation. p. 22. Federation of Small Businesses response to November 2023 Illegal Harms Consultation, p. 5. Google response to November 2023 Illegal Harms Consultation, p. 66. Nexus response to November 2023 Illegal Harms Consultation, p. 23. Stop Scams UK response to November 2023 Illegal Harms Consultation, p. 20. Yoti response to November 2023 Illegal Harms Consultation, p. 20.

[8] OnlyFans response to November 2023 Illegal Harms Consultation, p. 12.

[9] Protection Group International response to November 2023 Illegal Harms Consultation, p. 14-15.

[10] New Zealand Classification Office (Te Mana Whakaatu) response to November 2023 Illegal Harms Consultation, p. 9.

legalistic language is often necessary to properly represent the associated laws to which service providers are required to refer. While we acknowledge that the ICJG is long and detailed, we do not believe it is possible to produce a shortened summary version which does not, in being shorter, misstate the law or give a misleading impression to providers.

2.17 In response to the concerns raised we have worked to simplify and clarify terminology where possible in our final ICJG, and have reviewed language to make it clearer, concise and more accessible where this does not compromise legal accuracy. Ofcom is committed to promoting and supporting compliance among service providers of all sizes. Over the coming months, we will work with providers to ensure that they can access the resources they need to understand and comply with their duties under the Act.

Reasonable grounds to infer threshold and risk of under-takedown

2.18 In our November 2023 Consultation, we did not propose to define 'reasonable grounds to infer', beyond noting that it is a new legal threshold which is different from the 'beyond reasonable doubt' threshold used by criminal courts. Instead, we stated that what amounts to reasonable grounds to infer in any given instance will necessarily depend on the nature and context of the content being judged and, particularly, the offence(s) that may be applicable.

2.19 In its response, the **Online Safety Act Network (OSAN)** was critical of Ofcom's approach to the 'reasonable grounds to infer' threshold, arguing that it had been set too high and is equivalent to a criminal threshold.[11] It advocated a 'balance of probabilities' threshold stating that reasonable grounds to infer exist where there is no countervailing benefit to the content being posted. The **Molly Rose Foundation** expressed concern that the ICJG 'inevitably focuses' on the freedom of expression risks associated with content takedown and adopts a burden of proof that is closer to a criminal than civil or regulatory regime. It argued this creates a risk that service providers will adopt a high bar before they consider content illegal and remove it.[12]

2.20 The reasonable grounds to infer threshold is the threshold set in law. As set out in our November 2023 consultation, we agree that it is not a criminal threshold, and we do not consider that the proposals on which we consulted involved the application of a criminal threshold.[13] However, we have no powers to depart from the definition set out in the Act, which requires there to be "reasonable grounds" to infer that "all elements" necessary for the commission of the offence concerned are present.

2.21 What amounts to reasonable grounds to infer in any given instance will necessarily depend on the nature and context of the content being judged and, particularly, the offence(s) that may be applicable. The potential impact of error on freedom of expression also varies from offence to offence. In certain circumstances where the risks of under-takedown are particularly high – namely in relation to child sexual exploitation and abuse offences – we have made it clear when service providers should treat content as illegal (in the case of user-to-user ('**U2U**') services, this requires content takedown). We do not, however, believe that such an approach is appropriate or proportionate in relation to all offences. In some cases there may not be *any* grounds for an inference to be drawn, which would be inconsistent with the definition set out in the Act. In others, the elements of an offence may

[11] OSAN response to November 2023 Illegal Harms Consultation, pp. 25-26.
[12] Molly Rose Foundation response to November 2023 Illegal Harms Consultation, p. 35.
[13] See, for example, paragraph 26.14 to 26.15, and 26.39 to 26.68.

be partially met but there may be significant uncertainty about offline elements of the offence such as state of mind or context. We take the view that the benefits to society of people being able to express themselves freely including online are important in and of themselves. An approach which leads to very large quantities of legal activity being deemed illegal because a small proportion of it *could* be illegal would not be appropriate.

Freedom of expression and risk of over-takedown

2.22 Several respondents raised concerns about the impact of the ICJG's proposals on freedom of expression (**Big Brother Watch, Name Withheld 3, SPRITE+ (University of Sheffield)**) with many (**Humanists UK, Global Partners Digital, Google**, **New Zealand Classification Office**, **X Corp**) saying that it risks removal of non-illegal content.[14]

2.23 We acknowledge the concerns raised by stakeholders in relation to freedom of expression. We consider that concerns primarily arise not from the draft ICJG but from the definition of illegal content itself, which is statutory.

2.24 We have considered freedom of expression questions throughout our drafting and, where these questions arise, have sought to balance the implications of our approach on freedom of expression with a full consideration of risk of harm. We have always considered our requirement to carry out our duties in a way that is compatible with the Human Rights Act 1998 and Article 10 of the European Convention on Human Rights (ECHR). Service providers also have a duty to have regard to the right to freedom of expression within the law. Ultimately, however, provided that it is complying with the Act, it is open to a provider in the exercise of its own right to freedom of expression to determine what content it wishes to allow on its service, and Ofcom has no power to prevent this. Furthermore, there is nothing in the Act that requires service providers to make illegal content judgements, so long as the application of that service provider's own terms and conditions is sufficient to secure compliance with the duties in the Act in other ways.

2.25 In its submission to our August 2024 Further Consultation on torture and animal cruelty, **Google** argued that is only 'reasonable to infer' illegality "when it is also 'reasonable to infer' that a court would do so.'[15]

2.26 'Reasonable grounds to infer' is entirely new legal threshold which is not the same as the thresholds used to date by UK courts in relation to these offences, and which we consider must be lower than that criminal threshold. In coming to this view, we have considered sections 59 and 193 of the Act and the overall purpose of the Act to regulate internet services, including the provisions which make it clear that Parliament envisaged that judgements may be made using automated technologies.[16]

Reasonably available information

2.27 Section 192 of the Act states that illegal content judgements "are to be made on the basis of all relevant information that is reasonably available to a provider".

---

[14] Big Brother Watch response to November 2023 Illegal Harms Consultation, p. 11. Google response to November 2023 Consultation, p. 67. Global Partners Digital response to November 2023 Illegal Harms Consultation, pp. 24-25. Humanists UK response to November 2023 Illegal Harms Consultation, pp. 15-16. Name Withheld 3 response to November 2023 Illegal Harms Consultation, p. 22. New Zealand Classification Office response to November 2023 Consultation, p. 9. SPRITE+ (University of Sheffield) response to November 2023 Illegal Harms Consultation, p. 22. X Corp response to November 2023 Illegal Harms Consultation, p. 4.

[15] Google response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 3.

[16] See section 192(3).

2.28 At consultation, we proposed providers will need to consider what information is reasonably available on a case-by-case basis as what may be relevant and reasonably available for the illegal content judgement may differ depending on the type of content, the offence it may amount to, the provider's Term of Service or Publicly Available Statement, and what other information is available. We gave examples of types of reasonably available information which might be relevant in different contexts, including: content information, complaints information, user profile information, user profile activity (in some cases) and published information from external sources.

2.29 In relation to automated systems and processes, the main automated technology we were proposing to recommend in Illegal Content Codes was for various kinds of content-matching (though we noted that it remains open to services to use such technologies, pursuant to their own Terms of Service or Publicly Available Statement). We therefore proposed a 'technology-agnostic' approach to both reasonably available information and content judgements in general.

2.30 We proposed that, when making illegal content judgements, service providers should continue to have reasonable regard to any other relevant information to which they have access, above and beyond what is set out in the ICJG but only so long as this information is processed lawfully, and aligns with data protection laws.

Clarity regarding what types of reasonably available information is required in each case

2.31 **LinkedIn**, **Lloyds Banking Group**, and **Nexus** broadly agreed with our assessment of what reasonably available information may include, including the principle that it should be both reasonably available *and* relevant to content judgements.[17] However, many respondents remarked on a lack of clarity regarding the reasonably available information which was required in each case. Respondents such as **Airbnb** and **Booking.com** argued that our definition was too broad and in need of clearer demarcation.[18] In its response, **Meta** expressed concern that the definition of reasonably available information was too broad and that due to its global scale, the volume of content for review is such that it would be disproportionate to require it to collect superfluous information to make an assessment. It therefore advocated for an approach that takes into account the technical specifics of different services.[19]

2.32 We never intended the list provided in the introductory section to suggest that a provider should have regard to every type of information listed in every case. In order to be clearer, we have introduced summary boxes after each offence which set out the information we consider to be reasonably available for the purposes of making judgements in relation to those offences. These boxes are derived from the text we had about each offence but have been updated for changes we made because of consultation. These boxes replace the section in our Introduction which sets out different types of reasonably available information in general terms.

2.33 We acknowledge that applying the ICJG at a global scale within a content moderation function is not necessarily straightforward. We note that at present, we have not made recommendations that providers should use proactive technology to detect suspected

[17] LinkedIn response to November 2023 Illegal Harms Consultation, p. 20. Lloyds Banking Group response to November 2023 Illegal Harms Consultation, p. 11. Nexus response to November 2023 Consultation, p. 23.
[18] Airbnb response to November 2023 Illegal Harms Consultation, p. 22. Booking.com response to November 2023 Illegal Harms Consultation, p. 12.
[19] Meta response, November 2023, pp. 37-38.

illegal content and we expect that the more complex judgements concerned will be made mostly in relation to complaints from UK users or affected persons, and trusted flaggers. We do not currently have the evidence we would need to take a view on what is proportionate for providers to consider when such judgements are made at a global scale. In particular, we would need evidence of costs. We may need to revisit our ICJG as the regulatory regime develops and we acquire more information.

2.34 For now, we have sought to keep the matters which providers must consider to a proportionate level. However, it must ultimately be presumed that Parliament intended most priority offences to be capable of giving rise to illegal content in some form, even though many of them involve elements which cannot necessarily be inferred from the content alone. It would therefore be inconsistent with the Act for us not to consider what information a service provider might reasonably have available which is probative of the offences concerned.

2.35 Conversely, we are also bound by our duties in relation to freedom of expression. Absent further evidence, we cannot give guidance that says providers need not consider information we know is readily available to them, which may show that content is not illegal.

2.36 We note that those who objected to the information we considered to be reasonably available did so at a high level and without any of the detail we would have expected to see from well-resourced and sophisticated entities who considered a proposal on which we were consulting to be significantly problematic for their business. They did not discuss individual offences, nor provide any substantive information as to why our proposals were untenable, nor did they make any suggestions as to how we should otherwise comply with our duty to give guidance on these matters consistently with the definition of illegal content in the Act. We infer from this that they are not, in practice, significantly burdened by our proposals. We therefore for the most part retained the same approach to that in our consultation regarding what information we considered to be reasonably available in relation to each kind of harm. Should evidence become available in the future which leads us to believe that this decision could be better balanced, we may review this guidance.

Expansion of standard reasonably available information

2.37 In its response, the **Canadian Centre for Child Protection (C3P)** argued that the list of types of information that could be considered both relevant and reasonably available should be expanded to include information about networks and connections, and comments or posts made by other users.[20] While we acknowledge that these pieces of information *may* be relevant, we see significant human rights risks in suggesting that inferences about illegality can be drawn based on who a user is networked with or connected to, and we do not have evidence on which to base guidance in this regard. Similarly, although we recognise that other users' comments may sometimes be of use, generally, we do not consider it would be proportionate to steer providers to consider such information as its value for helping the provider to draw inferences about a different user's conduct or state of mind would usually be limited. Asking providers to look at either type of information would amount to an interference with the privacy of both the user posting and users connected to them, and would potentially place a significant burden on services when making content judgements. Overall, at present, we do not consider that this would be proportionate.

[20] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 34.

2.38 The **Online Safety Network** similarly argued that inferences ought to be drawn from patterns of posting in some cases as well as the context of content surrounding the post.[21] It also suggested that Ofcom should consider where metadata is appropriate too. We have considered these points on a case-by-case basis and have updated relevant sections with these types of information. We are not recommending any user behaviour pattern detection technology in our Codes of Practice and therefore do not think we can recommend that this sort of information is reasonably available to providers. At this stage, we do not have evidence as to its value in drawing inferences about illegality. On the wider point regarding context, it would pose a serious risk to user privacy if service providers were to consider *all* contextual information which could be gleaned from a user's posting activity. We therefore believe our current approach is proportionate given these risks.

Illegal content judgements and data minimisation

2.39 In its response, the **Information Commissioner's Office (ICO)** noted that making illegal content judgements is an area of potential tension between online safety and data protection law, particularly in relation to the principle of data minimisation.[22] The **ICO** also pointed out a potential discrepancy between wording in paragraph 26.27 of our November 2023 Consultation document (Volume 5) and wording on the same matter in the ICJG itself at paragraph A1.67. It suggested that the wording in the ICJG was 'phrased more equivocally' and expressed for the text from Volume 5 to appear in the ICJG itself. It furthermore suggested that the text should clarify "that services may not always need to consult all available information in every instance, if it is possible to make an accurate judgement using less information."[23]

2.40 We have made sure to stress the importance of the data minimisation principle in sections of the ICJG where we ask providers to look at the wider context surrounding a piece of content. We note that in most cases, the most relevant information to be considered is the content itself and any information provided by third parties regarding the content (for example, through the free text box in a report). Where we have suggested that further information is reasonably available, we believe it is justified by the nature of the offence and/or extent of the harm concerned. For example, we believe it is reasonable to ask providers to look at more information when considering potential terrorism offences because there is potential for serious harm, but also very significant impacts on freedom of expression if content which does *not* amount to this offence is wrongfully removed.

2.41 Regarding the ICO's suggestions in relation to paragraph A1.67, we accept this suggestion and have amended our guidance accordingly. This text can be found at paragraph 1.65 in the final ICJG.

2.42 In its response, the **British and Irish Law, Education and Technology Association (BILETA)** also raised concerns about potential threats to data protection. It argued that, in practice, services will use behaviour monitoring technology to comply with the guidance despite Ofcom's decision not to define such information as "reasonably available."[24] **BILETA** also said that it did not believe that Ofcom's statement that data can be processed "only so long

[21] OSAN response to November 2023 Consultation, p. 24.
[22] ICO response to November 2023 Illegal Harms Consultation, p. 23-24.
[23] ICO response to November 2023 Illegal Harms Consultation, p. 24-25.
[24] British and Irish Law, Education and Technology Association (BILETA) response to November 2023 Illegal Harms Consultation, p. 22.

as [the] information is processed lawfully, including in particular in line with data protection laws" is sufficient, given the details of requirements set out in the Guidance.

2.43 In response, we note that we are not able to control what service providers choose to do to comply with the Illegal Content Judgments Guidance, and can only recommend what we believe is the appropriate approach which will allow providers to be in compliance with their duties under the Act while also minimising negative implications for data and privacy. Regarding the sufficiency of our drafting on processing data in line with data protection laws, we note that the Illegal Content Judgments Guidance cannot provide comprehensive advice on what the best practice relating to data processing is. We believe the ICO is best placed to do this, and have referred service providers to ICO guidance where appropriate.

Risk assessment and safety duties for content of which a provider is not specifically aware

2.44 In our consultation, we drafted on the basis that if a provider knows what illegal content is in relation to judgements about individual items of content, it will also know enough to be able to carry out risk assessments and meet the safety duty in relation to that kind of illegal content. We included cross references to our proposed Register of Risks in order to explain to service providers how the harms might manifest on providers of different kinds.

2.45 Having considered the size and capacity of services, we proposed to take the view that while an average or larger service provider may have access to information that a micro-business does not, such information was not relevant to a content judgement about the illegality of a single piece of content. Reasonably available information for an average or larger service, that is relevant to an illegal content judgement, would also be reasonably available to the smallest services.

2.46 In its response, the **OSAN** argued that our approach to the ICJG "focuses primarily on individual items of content and assessing whether content should be taken down", largely ignoring "the Act's systemic language" and the principles of safety by design.[25] It commented that Ofcom should also consider what the signals for inference about the mental element of crimes under section 192 are in relation to systems design – the examples it gave were patterns of posting in the context of harassment and 'the existence of networks'.[26] The **Center for Countering Digital Hate** similarly argued that the ICJG should apply a "systems-focused approach" and use "the systemic language and proportionate system design obligations also contained in the Act."[27] Similar points were made by **Refuge** and an individual.[28] The **OSAN** furthermore noted the relationship between a safety-by-design approach and moderation at scale.[29]

2.47 We note that our draft ICJG included references to the Register of Risks. Considering the responses already summarised, we have revisited our guidance to draw out further the types of illegal content which may need to be considered for the purposes of risk assessment. However, for most offences, there are so many ways in which illegal content could manifest that we do not consider it helpful to providers to give detailed guidance for

[25] OSAN response to November 2023 Consultation, p. 20.
[26] OSAN response to November 2023 Consultation, Annex D pp. 5-6.
[27] Center for Countering Digital Hate (CCDH) response to November 2023 Illegal Harms Consultation, p. 12
[28] Refuge response to November 2023 Illegal Harms Consultation, p. 25. McGlynn, C. response to November 2023 Illegal Harms Consultation, p. 14.
[29] OSAN response to November 2023 Consultation, pp. 20, 23

the purposes of risk assessments in the ICJG. Service providers will be better placed to consider this for themselves in the light of the offences concerned.

2.48 On the specific examples given, we consider that our guidance on harassment is clear that one way in which harassment may be committed is by repeated attempts to impose unwanted communications and contact. However, we do not have evidence of how user behaviour patterns in relation to harassment differ from user behaviour patterns in relation to political activism, commercial activities, dating or other benign forms of conduct. In our view, and as set out in our ICJG, complaints about harassment are likely to be particularly important in bringing providers' attention to it.

2.49 Based on the evidence we have at this early stage in the establishment of the regulatory regime, we do not consider that it would be consistent with users' rights to privacy or freedom of association for us to give guidance suggesting that providers should draw inferences about illegality based on who a user is connected to. Such an approach would impact not just the rights of the user in question, but all users.

2.50 More generally, we do not consider it appropriate to give guidance suggesting that information is 'reasonably available' where we are not in a position to assess the rights impacts, personal data impacts, accuracy, effectiveness or freedom from bias of the technologies that providers would need to use to acquire such information. At this stage, for the most part, we do not have any evidence on when metadata indicators might help give rise to reasonable grounds to infer that content is illegal.

2.51 It is true that the online safety regime is a systems and processes regime. Ofcom recognises the need for service providers to take such an approach to the management of online harm, including harm from illegal content. The ICJG is one piece of a much larger regulatory scheme to address how illegal content can be properly assessed and managed, including at scale. It would not be right, however, to give guidance suggesting that providers should take steps to comply with the safety duty, which we are not able to say are proportionate and could not include in Codes of Practice. Such guidance would also be futile as it could not be enforced. Measures to comply with the safety duty belong in Codes.

References to law enforcement and third parties

2.52 As part of our wider proposals on reasonably available information, the draft ICJG proposed that information from law enforcement would be relevant to several offences. In the context of controlling a prostitute for gain, we suggested that a provider would be likely to need information from a credible third party (like for instance law enforcement) to make a reasonable inference about whether the person posting the content is or is not the same individual whose sexual services are being advertised. In other instances, we suggested information from law enforcement would be contextual rather than determinative (for example, if law enforcement provided information on a user exposing a gun for sale). We also proposed to steer services to respond to content amounting to a relevant non-priority offences where they have been made aware of it by law enforcement.

2.53 **X Corp** stated that the ICJG would benefit from explaining the factors that platforms should consider to discharge their freedom of expression obligations when considering non-legally binding requests to remove content (for example, requests from law enforcement authorities and regulators).[30] Service providers are not required to perform the same type

[30] X Corp response to November 2023 Consultation, p. 3.

of freedom of expression analysis where they are legally compelled to remove content by a court order.

2.54 We acknowledge the concern raised and have decided to add new drafting in relation to almost all offences which states: "A provider is not required to accept the opinions of a third party as to whether content is illegal content. Only a judgement of a UK court is binding on it in making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided."

2.55 The exception is in the case of offences from the Financial Services Markets Act, our view that it is appropriate to steer services to rely on information from the Financial Conduct Authority (FCA) in relation to certain priority offences. As set out in our November 2023 Consultation, these offences are complex enough that we consider it unlikely that content moderators can be expected to understand and apply them correctly. The FCA has very significant expertise in this area and is itself bound to act consistently with human rights. We therefore consider that our approach lowers the risk of legal content being judged illegal, which is more compliant with Article 10 than providers attempting to do this themselves.

Addition of animal cruelty and human torture offences

2.56 At a late stage in the progression through Parliament of the Bill which became the Online Safety Act, the offence in section 4(1) of the Animal Welfare Act 2006 (unnecessary suffering of an animal) was added to it. We decided to consult separately on how we propose to include that offence in our guidance, and published our consultation on Protecting people from animal cruelty and human torture content online in August 2024. Responses to that consultation are set out along with our decisions (see paragraphs 2.352 to 2.378).

Reference to non-priority offences

2.57 At consultation, we proposed to focus the ICJG primarily on priority offences, except in cases where offences were created by the Act or were particularly likely to result in illegal content. In practice, this meant we gave substantive guidance on only four non-priority offences: the self-harm offence, cyberflashing offence, epilepsy trolling offence, and false communications offence.

2.58 In our August 2024 further consultation on torture and animal cruelty ('**August 2024 Further Consultation**'), we proposed to extend our guidance to include a particular aspect of the offence in section 127 of the Communications Act 2003 (the '**s. 127(1) offence'**), in order to capture obscene content (in the sense of being atrocious and horrific) such as animal and human torture. We explained in that consultation that, at this early stage in the establishment of the regulatory regime, we did not consider it proportionate to say that service providers should build their systems and processes to enable them to consider all potentially relevant non-priority offences as well as priority offences, where a priority offence already exists targeting the type of content concerned. Parliament chose to define certain offences as priorities.

2.59 In particular, we did not think that we should include non-priority offences in our regulatory products where there is not a clear gap in the type of content covered. We also thought the risks to freedom of expression if we give specific guidance on too many aspects of the s. 127(1) offence to be very high even with our guidance, because the terms used in it are too

broad and so have a high risk of being misunderstood by those who are not experts in UK laws.

2.60 Providers would need to make judgements about content said to amount to an offence in relation to which we did not provide guidance, in accordance with Chapter 16 of the ICJG.

Use of s. 127(1) of the Communications Act

2.61 Many stakeholders welcomed our use of the s. 127 offence in principle. These included **Battersea Dogs and Cats Home, Blue Cross**, **Google/YouTube**, the **OSAN** and **SWGfL**.[31] However, there were concerns raised about our approach.

2.62 The **RSPCA** and **Scottish SPCA** raised concerns that the approach "may confuse enforcement agencies particularly those with limited access to legal expertise."[32] The **RSPCA,** the **Born Free Foundation, International Cat Care** and **Scottish SPCA** also noted the lack of successful prosecutions under s. 127 regarding animal cruelty.[33] The **RSPCA** further argued that the language in the Communications Act 2003 is "too vague to be used for animal cruelty prosecutions" and is therefore not a "suitable tool" for animal cruelty prosecutions, saying that it is "that the monkey torture case used the Obscene Publications Act 1958 to successfully prosecute rather than the Communications Act 2003 [s. 127(1)], possibly for the same reason."[34] **SMACC** (Social Media Animal Cruelty Coalition) raised a concern that "considering cruelty content as a 'non-priority offence' is effectively downgrading such content, which may cause it to be treated as less serious by online services."[35] The **Born Free Foundation** similarly expressed concern that the reliance on the s. 127(1) offence will create "a significant risk that platforms will not prioritise such content for removal."[36]

2.63 We recognise this concern. However, we have to work within the framework of the legislation. Indeed, by providing specific guidance on the s. 127(1) offence in relation to animal cruelty, even though the s. 127(1) offence is not a priority offence, we have indicated how seriously Ofcom takes animal cruelty content.

2.64 Whether content is illegal because of a priority offence or a non-priority offence, a provider must have proportionate systems and processes to take it down once it is aware of it.

2.65 Regarding the **RSPCA**'s, **Scottish SPCA**'s, **International Cat Care** and **Born Free Foundation**'s comments regarding criminal prosecution: it is not necessary to meet the criminal threshold when judging content to be illegal content, and criminal prosecutions take place entirely

---

[31] Battersea Dogs and Cats Home response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 9. Blue Cross response to August 2024 Further Consultation on Torture and Animal Cruelty, pp. 5-6. Google YouTube response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 3. OSAN response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 4. SWGfL response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 6.

[32] RSPCA response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 10. Scottish SPCA response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 7.

[33] Born Free Foundation response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 5. International Cat Care response to the August 2024 Further Consultation on Torture and Animal Cruelty, p. 5. RSPCA response to August 2024 Further Consultation, p. 10. Scottish SPCA response to August 2024 Further Consultation, p. 7.

[34] RSPCA response to August 2024 Further Consultation, pp. 6-7

[35] SMACC response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 7.

[36] Born Free Foundation response to August 2024 Further Consultation, p. 4.

separately, unaffected by the Act and the process of making content judgements. Law enforcement agencies did not object to our approach.

2.66 The **OSAN**, while welcoming our inclusion of the s. 127(1) offence in principle, called for the offence to be applied more broadly in relation to other offences.[37] This is something we have considered, as set out in Annex 6 to our August 2024 Further Consultation, but we believe the freedom of expression risks of a broader application of the offence are too significant to justify further widening of the scope. We believe that, for the reasons set out in paragraph 2.60, it is proportionate to use the s. 127(1) offence with reference to human torture and animal cruelty content, but that this cannot be said for other harms areas.

2.67 We have therefore decided to refer to the s. 127(1) offence *only* in relation to human torture and animal cruelty content, and to otherwise go forward with our original proposal to refer to non-priority offences only when these offences have been created by the Act.

2.68 We acknowledge that this means that several of the examples given by stakeholders are unlikely to amount to illegal content as they neither encourage, assist or conspire to an offence under the Animal Welfare Act 2006 (see 'Animal Cruelty' section, paragraphs 2.352-2.378), nor do they reach the threshold to be considered 'obscene.' This includes examples raised by **SWGfL** and **Battersea Dogs and Cats Home** content depicting acts such as posting images of hunting dogs after a hunt, tickling a slow loris, 'trend' videos such as barking at dogs or wearing masks to scare pets, walking cats on leads, dressing up animals in human clothes and others.[38] We note, however, that many of these acts are not in themselves illegal.

Provision of content examples

2.69 Several responses, including responses from [✂] and **Federation of Small Businesses**, suggested that Ofcom should test our guidance on pieces of actual content to ensure that it works, or else provide case studies that would illustrate how to apply the ICJG to content in practice.[39]

2.70 We have considered how the ICJG can be applied to real-life examples of content as part of our policy development process. We considered whether to give examples of content in the ICJG, but decided against it. The ICJG is already lengthy, and it would not be possible to give a sufficiently large number of examples to be useful in practice without increasing the length hugely. By giving examples, we would risk encouraging a simplistic black-and-white approach to content which was (on its face) similar to the examples given.

Applicability of guidance to search services

2.71 In its response, the **OSAN** criticised the ICJG for being overly concentrated on U2U services, and not providing adequate guidance for use by search services.[40] It should be noted that we did not receive any concerns of this kind from search services themselves.

2.72 We acknowledge that the draft ICJG – though neutral in its stance towards the type of service being considered – reflected the higher and richer amount of reasonably available information available on U2U services. We have therefore added separate boxes (where

[37] OSAN response to August 2024 Further Consultation, pp. 4-5.
[38] SWGfL response to August 2024 Further Consultation, p. 2. Battersea Dogs and Cats Home response to August 2024 Further Consultation, p. 12.
[39] [✂]; Federation of Small Businesses response to November 2023 Consultation, p. 5.
[40] OSAN response to November 2023 Consultation, p. 22.

appropriate) detailing the reasonably available information which should be considered by providers of U2U services and search services respectively. We have also added further information on how services should use the ICJG in our introductory chapter.

2.73 In addition, we have reviewed our wider chapters and adapted our approach to take greater account of search services and the information available to them. In particular, we have concluded that content amounting to the following offences is unlikely to be found in search results except where they contain a link to a U2U website: cyberflashing, epilepsy trolling, harassment, stalking and coercive and controlling behaviour. In most cases, this is due to the need to make inferences about intent, and the targeted nature of the content. We have therefore decided to add drafting to the respective chapters which states that these offences are to be considered by search services only to the extent that content on U2U services appears in search results.

Model terms of service

2.74 At consultation, we acknowledged that service providers may meet their duty regarding removal of illegal content by having and applying terms of service which encompass all illegal content under the Act. Stakeholders were in general supportive of this. **SPRITE+ (University of Sheffield)** said that it would be helpful if Ofcom mapped terms and conditions of a number of services (both large and small) against the ICJG so that it would be easier for services to see where adjustments were needed.[41] We do not believe it would be appropriate to do this, as providers' terms and conditions of service are specific to them.

Inchoate offences

2.75 Inchoate offences happen when someone is involved in another offence in a way which makes them guilty, without actually committing the offence themself. For example, a person may 'assist' in a robbery if they drive the getaway car. They did not carry out the offence, but they were involved in it. It is our provisional view that the most common ways in which an inchoate offence might be committed online are by encouraging or assisting a priority offence or by conspiring (that is, making an agreement) to commit a priority offence.

2.76 To produce guidance that is timely and move forward with the regime at pace, the draft ICJG contained relatively little detail in relation to inchoate offences. Broadly speaking, our proposals touched on inchoate offences only where it was clear that the base offence would be unlikely to result in illegal content. Having had additional time to consider this issue, however, we have revisited the inchoate versions of each priority offence, and have assessed whether additional guidance is needed. We have also added more on the Scottish inchoate offence of being involved art and part in the commission of a priority offence.

Use of URL links

2.77 In the draft ICJG, we touched on how providers should approach URL links in illegal content only in relation to child sexual abuse material (CSAM) offences and the epilepsy trolling offence, in which we argued that a link to an illegal CSAM image or video, or a flashing image, should be considered as illegal content in itself. We have added some further examples of offences in relation to which a URL linking to content may in itself be illegal

[41] SPRITE+ (University of Sheffield) response to November 2023 Consultation, p. 21.

content. These relate to terrorism, drugs, image-based adult sexual offences, and encouraging or assisting suicide.

Jurisdictional considerations

2.78 As set out in our November 2023 Consultation, the priority offences outlined in the Act include offences from each of the three different UK jurisdictions: England and Wales, Scotland, and Northern Ireland. The Act states that "[f]or the purposes of determining whether content amounts to an offence, no account is to be taken of whether or not anything done in relation to the content takes place in any part of the United Kingdom." The Explanatory Note to the Act explains that the effect of this is that "content does not need to be generated, uploaded or accessed (or have anything else done in relation to it) in any part of the United Kingdom to amount to an offence under this provision. This is the case regardless of whether the criminal law would require the offence, or any element of it, to take place in the United Kingdom (or a particular part of it).

2.79 We consider that the practical impact of jurisdictional differences is limited due to significant overlap between laws in the United Kingdom's three jurisdictions. However, we identified isolated cases in which a priority offence in one part of the United Kingdom is different from other jurisdictions. Where this is the case, we have set out an appropriate approach to be taken in the Guidance chapter concerned.

2.80 The same logic applies if the content is posted outside of the UK. However, the interpretative rule in the Act applies only to what happens in relation to the *content* posted. It does not affect, for example, any offline circumstances required for the offence to be committed. We consider, for example, that the word 'sale' which is used in several priority offences, should be construed as sale to persons in the UK unless the underlying priority offence has extra territorial effect. Similarly, for any inchoate offences to be committed, the offence being encouraged, assisted or conspired to etc would need to be an offence within the territorial jurisdiction of the UK.

Updating the ICJG

2.81 We recognise that there is the scope for further changes to the Act, and that case law in relation to existing offences is also likely to change, meaning the ICJG will need updating. To mitigate any risk associated with incorrect or incomplete information, we will review and update the ICJG periodically, consulting on changes where necessary.

2.82 We believe this will also address concerns raised by **Battersea Dogs and Cats Home** regarding the potential for bad actors to change their behaviour when alerted to what is illegal in the ICJG, 'gaming the system' and therefore avoiding content removal.[42] We will continue to remain vigilant in regard to emerging trends in illegal content and will ensure that our guidance reflects these. We also believe this addresses the point raised by **Stop Scams UK** [43] regarding the need to evolve and update our guidance on fraudulent content.

Offence specific

2.83 In this section, we set out our decisions in relation to offence-specific proposals made at consultation. Due to the quantity of proposals made in the draft ICJG, we have outlined our reasoning in this section where we have made significant changes or received stakeholder

[42] Battersea Dogs and Cats Home response to August 2024 Further Consultation, pp. 9-10.
[43] Stop Scams UK response to November 2023 Illegal Harms Consultation, p. 20.

responses which require a detailed explanation in response. Other issues are outlined in the annex titled 'Annex 1 to the statement on Further stakeholder responses'. In the annex titled 'Annex to Volume 3' we set out our reasoning for the proposals which we have gone on to adopt in our ICJG without substantive changes.

2.84 We have decided to move all non-priority offences into a dedicated chapter on non-priority offences in order to make the differing expectations for risk assessment clearer to distinguish. In our rationale as set out in the following sections, however, non-priority offences are found under the section heading in which they were originally included in the draft guidance: epilepsy trolling in 'Threats, abuse and harassment (including hate); self-harm in 'Suicide and self-harm'); false communication in 'Foreign interference and false communications' and cyberflashing in 'Image-based adult sexual offences.' In addition, offences relating to animal cruelty and misuse of a public communications network are also found together, as these were consulted on at the same time.

Terrorism

2.85 We have reordered the guidance on the terrorism offences, to bring the easier to identify offences to the top. The terrorism offences comprise:

a) Offences related to information likely to be of use to a terrorist;
b) Offences relating to training for terrorism;
c) A series of offences relating to 'proscribed organisations';
d) Other offences involving encouraging terrorism or disseminating terrorist publications;
e) Miscellaneous, more specific terrorism offences; and
f) Offences relating to financing terrorism.

Reasonably available information for terrorist offences – who the person posting is

2.86 In relation to several of the terrorism offences, in our November 2023 Consultation, we took the approach that context was relevant to determining whether the conduct element of the offence was met. However, we said that the "full" or "whole" context was relevant, without particularising how, and so we did not particularly identify the person posting the content as a factor to consider. We took this approach to many of the proscribed organisations offences, dissemination of terrorist publications, encouragement of terrorism and incitement of terrorism overseas.

2.87 As set out in paragraph 2.32, respondents believed that it was not sufficiently clear what reasonably available information was to be considered in each case. As set out in paragraph 2.40, the ICO stated that it was necessary to consider data minimisation when considering the parameters for content judgements. The **Cyber Threats Research Centre at Swansea University** said our draft guidance to providers should consider the author of the content, and/or the identity of the user disseminating the content was insufficiently clear.[44]

2.88 In relation to our governance and content moderation proposals generally, the **Oxford Disinformation and Extremism Lab** highlighted the need for human rights advocates,

[44] Ofcom meeting May 2024, subsequently confirmed by Cyber Threats Research Centre at Swansea University, 28 August 2024. For the s.2 Terrorism Act 2006 offence, we consulted on usage examples including internet publications authored by known terrorists or known to be distributed by terrorist networks.

universities and research organisations, and researchers to remain able to continue their work.[45]

2.89 The work we have undertaken since consultation has demonstrated that assuming the conduct and state of mind elements of certain offences are met, based only on the content concerned, we could see significant amounts of lawful content of public interest being judged illegal. Research bodies, human rights groups, anti-terrorism organisations, and state bodies do publish, for example, copies of terrorist manifestos and information about proscribed organisations. In so doing, they are not likely to be committing the conduct element of offences such as belong to or inviting support for proscribed organisations, dissemination of terrorist publications or encouraging terrorism; and where it may appear that they have, its likely they would have a defence.

2.90 We recognise the importance of identifying who is posting or publishing the content to determining whether content is illegal. We accept that our proposed approach to these offences would have had a potentially significant impact on public interest research, safety and freedom of expression.

2.91 Giving guidance to providers that they should consider more information to make illegal content judgements imposes, of course, a cost upon them. This is because making the information available to content moderation could involve systems changes, and because where human moderators are used, each additional factor to consider involves a cost in initial training and then the time required to make a judgement about each item of content moderated.

2.92 However, we believe it is proportionate to ask providers to look at more information when considering potential terrorism offences because there is not only potential for very serious harm from this type of content being present, but also very significant threats to freedom of expression if content which does *not* amount to this offence is wrongfully removed. We consider that service providers which have content moderation teams are likely to have means of escalating such serious suspected illegal content to a dedicated team with access to more information.

2.93 In our final guidance, we have therefore added wording to explain when and how the identity of the user posting or the website author is relevant to illegal content judgements.

Reasonably available information for terrorist offences – other contextual information

2.94 In our draft ICJG, we noted that merely depicting terrorism is not illegal, and that providers would need to consider the purpose and meaning of content when making illegal content judgements, having regard to the whole context in which it appears.

2.95 The **Cyber Threats Research Centre at Swansea University** said we should add the following factors to our guidance:[46]

a) The wider pattern of consumption of the user posting the content, in line with domestic case law.

[45] Oxford Disinformation and Extremism Lab response to November 2023 Illegal Harms Consultation, pp. 8 and 10.

[46] Ofcom meeting May 2024, subsequently confirmed by Cyber Threats Research Centre at Swansea University, 25 August 2024.

b) Existing surrounding circumstances in which the online content is published or disseminated. For example, in the aftermath of a terrorist attack. This can be indicative of the potential and/or desire to lead to harmful consequences.[47]
c) The apparent purpose of the person making the statement/downloading the content, related to another factor considered in ECtHR case law: the manner in which statements in online content are made.[48]

2.96 We have decided not to steer providers to consider the wider pattern of consumption of the user posting the content, as we consider the potential human rights impacts and cost impacts of this approach to be too significant. We are not confident that, even with our guidance, most moderators would be able to make appropriate judgements about the relationship between content consumption patterns and a user's state of mind. We are concerned that to have regard to such information would be unnecessary in many cases but would lead to over-takedown in borderline cases. In the circumstances, we are not persuaded that the significant negative impacts on privacy or the extra costs to providers would be justified.

2.97 However, we agree that in some cases it is relevant for services to consider the "information readily available to them through taking appropriate steps to be informed of the immediate, publicly-known UK state of affairs in which the online content is published or disseminated (for example, a publication circulated in the aftermath of a particular event, which will most likely be reported by major international news outlets)." We believe such information is relevant to the following offences: information likely to be of use to a terrorist (where the information is otherwise benign), dissemination of terrorist publications, encouraging terrorism and inciting terrorism overseas. This is because sometimes the context in which information is posted is informative as to its meaning and purpose. We have therefore amended our guidance accordingly for those offences.

2.98 We have not included this factor as reasonably available information for the purposes of considering the offence of preparation of terrorist acts. This offence is a very broad one, so the omission is not because it is impossible for such information to be relevant. It is because we consider that it risks being disproportionate to ask providers to consider such information for an offence which will in any event be very difficult for them to identify save in circumstances involving proscribed organisations (for which it is less likely to be necessary to know about the current state of affairs).

2.99 We also agree that it is relevant to consider the apparent purpose of the person posting content in certain cases. For example, in the case of proscribed organisation offences encouraging terrorism, or dissemination of terrorist publications, it will not be appropriate to reasonably infer that content is illegal where it has been "posted to the website of an institution whose job it is to research and combat terrorism", or posted by "organisations and individuals, such as law enforcement authorities, anti-terrorism organisations, academic researchers, journalists and human rights organisations." We have therefore decided to amend our ICJG to draw this out.

[47] It noted the weight placed on this in human rights cases: Bidart v France App No 52363/11 (ECtHR, 12 November 2015), Stomakhin v Russia App No 52273/07 (ECtHR, 9 May 2018).
[48] Perinçek v Switzerland App No 27510/08.

Notices from a constable

2.100 Section 3 of the Terrorism Act 2006 provides for a 'constable' (a type of UK police officer) to give notice to service providers that content is unlawfully terrorism-related. When we consulted, we mentioned this in our draft guidance.

2.101 The **Independent Reviewer of Terrorism Legislation** responded suggesting we not include this, as the power has not been used and providers may be induced to believe that they need only identify content as illegal content when a notice has been served.[49]

2.102 We remain of the view that the information about the notices is likely to be useful to providers, many of whom may be unfamiliar with UK laws. The fact that the power has not been used to date does not mean it will not be used. We consider it is clear from the Act and our Codes that it would not be permissible for providers to identify terrorism content only when they receive a notice like this, but for the avoidance of doubt have added words to our guidance to make this explicit.

The definition of terrorism

2.103 A stakeholder responded to our consultation saying that the UK statutory definition of terrorism is too broad. It argued this may lead to an overly cautious approach by service providers, with negative effects on freedom of speech.[50]

2.104 Ofcom does not have any power to change the statutory definition of terrorism. Our guidance has been developed with freedom of expression in mind.

Order of offences

2.105 Some of the terrorism offences are likely to be much easier to make reasonable inferences about than others. Our final guidance steers providers to begin by considering the offences we think are likely to be least difficult to identify (principally offences with the lowest 'state of mind' requirements), rather than the offences that are most likely to occur.

2.106 We have changed the ordering of our final guidance to better reflect the ease of making illegal content judgements. This means the proscribed organisations offences now appear after the offences of collection of information likely to be of use to a terrorist and terrorist training.

Information likely to be of use to a terrorist

2.107 It is an offence to collect, make a record of, possess, view or access information likely to be of use to a terrorist. As noted in our November 2023 Consultation, the state of mind requirements for the offence are low (knowledge of what the content is) and although there is a defence of 'reasonable excuse', for the content to be lawful every person seeing the content would need to have a reasonable excuse.

2.108 In the draft guidance on which we consulted, we said that providers should consider whether the content is "information that is, of its very nature, designed to provide practical assistance to a person committing or preparing for an act of terrorism". We stated that content that may be useful to a terrorist, but which also has clear legitimate uses - for example a map or public transport information – would not be information 'likely to be of use to a terrorist'.

---

[49] The Independent Reviewer of Terrorism Legislation response to November 2023 Illegal Harms Consultation, p. 7.

[50] Cyber Threats Research Centre at Swansea University response, 2023, pp. 18-19.

2.109 In its response to our November 2023 Consultation, one stakeholder [✂][51] asked us to change some of our proposed drafting to describe the law more accurately, and we have done so as follows:

a) In our final guidance we do not use the word "designed", but now only refer to information that is likely to provide practical assistance to a person committing or preparing an act of terrorism;
b) We have added some examples of where otherwise innocuous information may, in context, become information likely to be of use to a terrorist: for example, if a terrorist posts a map with a target for attack marked on it, or transport information relating specifically to how to get to a targeted location or person.

2.110 We accept that this wording still narrows the offence somewhat. However, service providers are not courts. To be useful, our guidance must be written in a way which can be applied by people who are not legal experts, necessarily have incomplete information and are making decisions quickly. The entities we regulate include many with limited resources. We therefore consider it appropriate to give guidance which steers them to make suitable decisions in foreseeable cases, without over-takedown.

2.111 We have also added new paragraphs to the guidance relating to:

a) URLs, because of the particular risk of users sharing URLs that lead to terrorist content on a website or another U2U service (including shortened URLs) in order to evade moderation; and
b) the need to consider the immediately, publicly known UK state of affairs, in which the online content was published.

2.112 In our guidance, we explain that there is a defence of 'reasonable excuse' to this offence. We give journalistic or academic purposes as examples of a reasonable excuse. However, we have noted that an audience which is larger and/or more general is more likely to contain users who would not access the content for a specific, legitimate reason (that is, for journalistic or academic purposes) and it is therefore less reasonable to say that the user collecting the information had a 'reasonable excuse'. Similarly, each person accessing or viewing the information would need their own 'reasonable excuse'. Furthermore, any content made available outside a limited group has the potential to be shared and spread in a way which the user sharing the information originally cannot control.

Terrorist training offences

2.113 The offence of 'providing weapons training' covers content which, in and of itself, provides instructions or training in the making or use of various weapons. This offence is likely to be relevant outside the context of suspected terrorism, because it is triggered whether the training or instruction is being made available generally or to suspected persons, and there is no state of mind requirement. In our November 2023 Consultation, we said that due to the definition of illegal content in the Act, jurisdictional considerations are not relevant, but we noted that a defence is available if providers have reasonable grounds to infer that the user's action or involvement was wholly for a purpose other than assisting, preparing for or participating in terrorism. We proposed that evidence of clear non-terrorist purpose is most likely to arise in relation to firearms. It should be noted that providing weapons training for legal purposes, for example as part of a rifle club, is not illegal. However, providers are not expected to ask the users posting and users viewing the content about their purposes,

[51] [✂].

before making an illegal content judgement. In the case of 3D printing instructions for firearms, we came to the provisional view that it is unlikely that a provider would have reasonable grounds to infer that the purpose was wholly non-terrorist.

2.114 One stakeholder [✂] responded to our consultation pointing out that the defence to this offence applies even when the purpose of the person offering the training is wholly criminal – for example offering training for the purpose of armed robbery of a bank.[52] We recognise this point but consider it exceedingly unlikely that service providers will have information regarding criminal (but non-terrorist) intent, and we do not consider that in these circumstances there would be a very significant interference with freedom of expression even if providers were to go beyond what our guidance says and treat the content as illegal. We therefore do not consider that there is a need to add this point to our guidance. We have updated our guidance to include additional information in relation to the offences of encouraging, assisting and conspiracy to terrorist training.

Proscribed organisations offences

2.115 The proscribed organisation offences are fairly straightforward. The list of proscribed organisations is publicly available. However, the drafting changes we have made to put more emphasis on the nature of the person posting content (whether on a U2U site or a website) and draw out more clearly how that affects the analysis means that providers should need to consider carefully whether the conduct element of the offences is made out.

2.116 In our November 2023 Consultation, we proposed to say that service providers which are aware of logos, flags or other iconography associated with proscribed organisations should factor these into their content judgements where appropriate. This could be ascertained through in-house specialist teams or through engagement with third party organisations that maintain databases of such information. Services should also have due regard to any evidence about proscribed organisation iconography submitted to them by law enforcement.

2.117 At the time, we were not aware of any publicly available, reliable list of such articles, although we said we intended to keep this under review pending the production of any suitable resource. Since we consulted, we have identified some third-party organisations which we consider could be relied upon for this purpose:

a) Tech Against Terrorism's Terrorist Content Analytics Platform;
b) Kings' College London Repository of Extremist Aligned Documents; and
c) Jihadology.

2.118 However, we do not yet fully understand the costs implications, especially for smaller providers, of recommending that it is reasonable for them to use these databases, and nor have we yet ascertained whether the providers could scale sufficiently to meet demand from all the providers we regulate, or all of those likely to be at risk of terrorism content. We consider, in any event, that we would need to consult on making a change of this nature to our guidance.

2.119 In our final guidance, we have therefore kept the same approach, but we have mentioned these databases as possible sources of information which, if the provider is aware of it, could be used to inform illegal content judgements.

[52] [✂].

2.120 The state of mind requirements for several of these offences are for the most part low, often only involving knowledge of what the content is.

2.121 In cases where the requirement is recklessness or intent, a service provider is not able to interview the person posting the content. We note that judgements about whether the content amounts to a joke or a work of fiction, for example, are already part of the assessment of whether the conduct element is made out. We therefore consider it reasonable for service providers to infer intent from the conduct element of the offence. For example, the state of mind requirements for the offence of professing to belong to a proscribed organisation require intent to profess to belong to the proscribed organisation. In our view, once a service provider has inferred that content is not a joke, fiction, academic research or journalistic commentary, but is indeed professing to belong to a proscribed organisation, it can infer intent to do so. We take the same view of content which expresses an opinion or belief that is supportive of a proscribed organisation in a way which will encourage others to support a proscribed organisation. If a service provider is able to infer that both those things are true, then it must be reasonably apparent. Absent evidence to the contrary, and noting that the threshold for these judgements is lower than beyond reasonable doubt, we consider it is reasonable to infer that the person posting it also recognised that.

Dissemination of terrorist publications

2.122 The offence of dissemination of terrorist publications relates to a publication which either:

a) may be understood as an encouragement to terrorism; or
b) could be useful in terrorism acts, and has been made available for that purpose.

2.123 We have added a paragraph to our guidance which draws out more clearly that posting a URL may amount to the offence of dissemination of terrorist publications.[53]

2.124 For content to amount to the offence, a provider must have reasonable grounds to infer that the publication was posted in a location where it could be seen by at least one person who could possibly (as opposed to will probably or certainly) be encouraged by it to commit an act of terrorism, and that the user who posted it either intended or was reckless that this would happen.

2.125 In considering what would amount to reasonable grounds to infer this, we thought about the likelihood of people posting content of this nature without recognising the risk that a person might be encouraged by it to commit a terrorist offence.

2.126 We took the view that if a terrorist publication has been uploaded to a location that can be accessed by anyone (for example a website or social media profile accessible generally by other users), it is reasonable to infer that it may be seen by somebody who could be encouraged to commit, prepare or instigate terrorism, and that most users posting such content would recognise this. We therefore proposed to steer providers to remove such content whenever it has been posted in a location that is easily accessible by other users, absent relevant defences and dependent upon the satisfaction of the other elements of the offence.

2.127 The **Cyber Threats Research Centre at Swansea University** argued that our approach to the dissemination of terrorist publications offence focuses too much on the public or private

[53] See, for example, the case of Mohammed Alam, discussed in Max Hill QC, 2017. Responding to terrorists' use of social media: legislation, investigation and prosecution. [accessed 8th October 2024].

nature of content and how this may indicate that content is illegal. It started that this 'disregard[s] the importance of the context of the expression' in a way which could lead to an overly cautious approach by service providers, potentially resulting in over-takedown and a negative impact on freedom of expression.[54]

2.128 In assessing whether content could be understood as an encouragement to terrorism or as being made available for that purpose, we emphasised in our consultation that context was important. As set out in paragraphs 2.87 to 2.94, we have drawn this out further in our final guidance, to be clear that content is not a terrorist publication if, in context, that is not how it would be understood by a reasonable person.

Encouraging terrorism

2.129 The offence of encouraging terrorism refers to published statements to members of the public which amounts to a direct or indirect encouragement to some or all the members of the public to the commission, preparation, or instigation of acts of terrorism or Convention offences. In our final guidance, we have clarified some of our drafting in relation to this offence, to make the elements of this offence clearer.

2.130 This offence can only be committed where the content concerned has been 'published' to members of the 'public'. It is clear from section 20(3) of the Terrorism Act 2006 that 'public' can include a group access to which is conditional. It is clear from section 20(4) that 'publication' can include using a U2U service to enable or to facilitate access by the public to the statement.

2.131 We consulted on draft guidance in which we took the view that content posted to a site or forum which is accessible to anyone is, by definition, published to members of the public. We also proposed to say that a members-only group which may be joined or accessed by any user without prior approval from an administrator or similar should still be considered accessible to the public. We accepted that terrorist publications are often disseminated in closed groups, and that the definition we proposed suggests that publication to a group may be publication to the public where access to a group is conditional. However, we considered that, without detailed investigation and substantial interference with the privacy rights of the members of the group, together with case specific legal advice, providers are unlikely to be in a position to make nuanced judgements about whether publication to the 'public' has taken place when the content is being shared via a 'closed', invitation- or prior-approval-only group, or a private social media account where follow requests must be approved. We therefore consulted on the view that where content has been posted to such a group, a service will not usually have reasonable grounds to infer that content has been published to the public.

2.132 In response to our November 2023 Consultation, one stakeholder [✂] suggested that a group with significant 'vetting' requirements could also include members of the public, and be in scope of the offence.[55] We acknowledge that this is possible, but at this point, we are not satisfied that it would necessarily be appropriate to give guidance to providers that they should assume all posts to vetted groups are being published to 'members of the public'. However, asking providers to obtain further information to take a more nuanced view on this would be time-consuming and resource-intensive for service providers, and would pose very significant privacy issues.

---

[54] Cyber Threats Research Centre at Swansea University response to November 2023 Consultation, pp. 18-19.
[55] [✂].

2.133 In the context of needing to prepare workable guidance, we believe that it is most appropriate for now to say that a provider will not usually have reasonable grounds to infer that content is published to members of the public where it has been posted to a 'closed', invitation- or prior-approval-only group or to a private social media account where follow requests must be approved. However, we acknowledge the challenge posed by vetted groups, including where some providers may have information that allows them to infer the presence of members of the public in a vetted group. We will therefore return to this matter as our policy understanding develops.

Preparation to give effect to an intention to commit or assist others to commit acts of terrorism

2.134 Engaging in any conduct in preparation for giving effect to an intention of committing acts of terrorism or assisting others to commit such acts is an offence.

2.135 In our final guidance, we have clarified some of our drafting in relation to this offence, to be clearer that the offence is *preparing* to commit or assist acts of terrorism, rather than committing acts of terrorism.[56]

2.136 We remain of the view that the state of mind requirement for this offence means that it is difficult to conceive of online content which would be identifiable as amounting to it, without also amounting to one of the offences considered earlier in our guidance.

2.137 When we consulted, we said that the offence was particularly relevant for U2U services when considering an account which appears to be run for and on behalf of a proscribed organisation. We also consider it may be relevant for search services considering search content, and have amended the drafting accordingly.

2.138 This is because the definition of terrorism means that any action taken for the benefit of a proscribed organisation should also be considered to be an action taken for the purposes of terrorism. Setting up an account or website for a terrorist organisation may be one of the specific proscribed organisation offences – for example doing so may show that the user belongs to a proscribed organisation and the content posted may invite others to support a proscribed organisation. But where that is not the case, it is reasonable to infer that the account or website exists in preparation for doing things to benefit the proscribed organisation, and that content posted to it is posted for that purpose.

2.139 This means that search services may need to consider whether search content is content posted in preparation to do things for the benefit of a proscribed organisation, which may require them to consider whether the website in which the content is posted is illegal content. However, we consider that websites run by or on behalf of proscribed organisations are likely to be a very small proportion of the content coming to search services for moderation, while the harm such content is likely to do is very severe. We therefore do not consider this to be a disproportionate burden on search services.

2.140 The offence may also be relevant to services when considering content relating to proscribed organisations which does not obviously fall within one of the specific proscribed organisation offences.

[56] This is to address a concern raised by a stakeholder [✂].

Terrorist threats

2.141 In our final guidance, we have reduced what we consulted on saying about terrorist threats on the basis that an offence of this kind is likely to be illegal content because of one of the threat offences (see section on 'Threats, abuse and harassment (including hate)').

Terrorist finance

2.142 In the draft guidance on which we consulted, we commented that of the terrorist financing priority offences, only the offence of inviting someone to provide money or other property for terrorism may be committed online through the posting of content.

2.143 One stakeholder [✂][57] suggested we soften this wording. On review, we accept that in theory there may be ways to provide financing via regulated content, and have said instead that the most likely offences that providers may be able to identify are the offences of inviting someone to provide money or other property for terrorism.

Other terrorism offences

2.144 Our reasoning in relation to the other terrorism offences is set out in the annex titled 'Annex to Volume 3'.

Threats, abuse and harassment (including hate)

2.145 The priority offences which relate to threats, abuse and harassment overlap with one another to a very significant degree. For the purposes of this section of the ICJG (and as set out in more detail in the annex titled 'Annex to Volume 3'), we therefore approach them based on theme, rather than offence by offence. The themes are:

a) Threats (including hate), encompassing:

   i) threatening behaviour which is likely to cause fear or alarm
   ii) threatening behaviour which is likely to cause harassment or distress
   iii) threats which are likely to stir up racial hatred
   iv) threats which are likely to stir up hatred on the basis of religion or sexual orientation
   v) threats which may provoke violence

b) Abuse and insults (including hate), encompassing:

   i) abusive behaviour which is likely to cause fear or alarm
   ii) abusive behaviour which is likely to cause harassment or distress
   iii) abuse which is likely to stir up racial hatred
   iv) abuse which may provoke violence

c) Other content likely to amount to harassment (including stalking and controlling or coercive behaviour)

2.146 In addition to the decisions set out in this section, further decisions in relation to threats, abuse and harassment (including hate) offences can also be found in the annex titled 'Annex to Volume 3'. We also set out some reasoning on a potential non-priority offence, the section 127(1) offence, in paragraphs 2.352-2.359.

[57] [✂].

Threatening and abusive behaviour

Reasonable person threshold

2.147 A number of the offences relating to threatening and abusive behaviour involve a 'reasonable person threshold'; that is, a test of whether a reasonable person would suffer, for example, fear or alarm from certain behaviour (such as harassment).

2.148 In our chapter on threats, abuse and harassment, we explain that a reasonable person is someone "who is not of abnormal sensitivity", in line with the legal definition. In its response, one stakeholder, **X Corp**, questioned our use of this standard, saying that it can be highly subjective and prone to over-enforcement.[58] However, the 'reasonable person' standard is written into several offences covered in this chapter, and we refer to it only where this is required to properly reflect the law. While we recognise that different people may have different views about what is 'reasonable', we do not consider ourselves well placed to define it further and note that it works sufficiently well for juries to apply in a criminal context. Where it is not defined, providers should use their judgement and take full account of the contextual factors discussed in the chapter.

Freedom of expression, 'banter' and offensive content that is not illegal

2.149 In our November 2023 Consultation document, we noted that the right to freedom of expression is engaged by the guidance we are giving, and we consider it particularly strongly engaged by the offences related to threats, abuse and harassment (including hate). It is particularly important for Ofcom to have regard to the right to freedom of expression in considering the safety duty in relation to the offences relating to insults and abuse causing harassment or distress, because of the risk that an over cautious approach to these would lead to disproportionate takedown, including (for example) of political and religious discussion.

2.150 We stated that the right to freedom of expression has been held *not* to be engaged by content which is 'gratuitously offensive' but acknowledged that robust debate often involves the expression of highly emotive and sometimes offensive opinions which touch upon issues of, for instance, politics, religion or race.[59] Similarly, humour often involves controversial speech which some people might find offensive and consider to be hateful or abusive. The draft ICJG sought to balance these two sides of the equation, as does our final guidance.

2.151 In its response, **Protection Group International** sought clarity on what, or how and who will consider a threat, abuse or harassment, arguing that it's possible to view content that may be deemed one of these, but it can also be viewed as 'banter', especially when no context is applied.[60] As our guidance says, we accept that "Differentiating between abuse amounting to illegal content and friendly 'banter' which appears abusive, or robust but lawful debate, is likely to be particularly difficult in the absence of a user complaint providing more context to frame the content in question." It states at 3.11 (A.38 in the draft ICJG) that 'Content is not illegal merely because it is offensive, shocking or disturbing; nor because it is rude. Lawful content may express unpopular or unfashionable opinions about serious or trivial matters. Banter and humour, even if in poor taste to some or painful to those subjected to

---

[58] X Corp response to November 2023 Consultation, p.4.
[59] *Otto-Preminger-Institute v Austria* (1995) 19 E.H.R.R. 34; *Wingrove v United Kingdom* (1997) 24 E.H.R.R. 1; Gündüz v Turkey (2003) 41 *E.H.R.R. 5; Giniewski v France* (2007) 45 E.H.R.R. 23.
[60] Protection Group International response to November 2023 Consultation, p. 14.

it, is not necessarily unlawful." We do not think it is possible for us to go further than this in our guidance, at least at this stage. Illegal content judgements are complex, and providers will need to take difficult decisions which depend on the judgment of the person looking at the content in its context.

Hate speech and the Sentencing Act

2.152 There are several priority offences which relate to the incitement of hatred on the basis of protected characteristics. It is an offence to make a threat or be abusive in a way which is likely to stir up racial hatred, and to make a threat intended to stir up religious hatred or hatred on the grounds of sexual orientation.

2.153 As set out in our November 2023 Consultation, in our final guidance we only give substantive guidance on the Public Order Act 1986 offences of stirring up hatred on the basis of race, religion and sexual orientation. We do *not* provide separate guidance on the racially or religiously aggravated priority offences. This is because once a provider has established that the elements of the non-aggravated offence are present, it is not necessary to go on to consider whether the offence is racially or religiously aggravated. The provider should take down the content regardless. By way of example, making an illegal content judgement that content amounts to an illegal threat, for example, is easier than showing it amounts to an illegal threat which is racially or religiously aggravated. Therefore, if a service has already identified illegal content because, for example, it amounts to an illegal threat causing fear or alarm, there is no need to separately consider whether it is also illegal content because the offence is racially or religiously aggravated. It is noted that sometimes the characteristics or identity of the victim are relevant to how reasonable it is for them to feel fear, alarm, harassment or distress.

2.154 In its response, one stakeholder [✂] suggested that the ICJG mention disablist, transphobic and homophobic hate crime aggravation outlined in section 66 of the Sentencing Act 2020.[61] We recognise the point raised by the stakeholder and its relevance to hate crime in general. However, we note that the Sentencing Act doesn't create offences, just uplifts sentences for already existing offences. This means it is not relevant in judgements about whether content amounts to an offence, as by definition any content which merited reference to the Sentencing Act would have already amounted to a separate offence before invoking the uplift. To mention the Sentencing Act would risk readers incorrectly assuming that the protected characteristics covered in the Sentencing Act but not in the Public Order Act (disability and transgender status) are themselves the subjects of hate offences. It would also be inconsistent with our approach to racial and religiously aggravated public order and harassment offences, as outlined above. We have therefore decided to keep our approach the same in the final Illegal Content Judgement Guidance.

Definition of race in offence of stirring up racial hatred

2.155 As noted in paragraph 2.153, it is an offence to make a threat or be abusive in a way which is likely to stir up racial hatred. In the ICJG, we outlined a definition of 'race' which stated that race "refers a group of persons defined by reference to race, colour, nationality (including citizenship) or ethnic or national origins." In its response, one stakeholder [✂] alerted Ofcom to case law which establishes that words that are not specific to one race have been found to be sufficient to constitute inciting racial hatred.[62] R v. Rogers [2005]

[61] [✂].
[62] [✂].

EWCA Crim 2863 held that hostility demonstrated to foreigners because they were foreign could be just as objectionable as hostility based on a more limited racial characteristic. In this case the phrases 'bloody foreigners' and 'go back to your own country' were used towards Spanish women. In Attorney General's Reference No 4 of 2004 [2005] EWCA Crim 889; the use of the word 'immigrant' in its simple implication that a person was ''non-British' was specific enough to denote membership of a racial group. We thank the stakeholder for bringing this case law to our attention and have updated the ICJG to steer service providers to consider content containing broader statements of the nature discussed as possible illegal content.

Approach to other harassment and coercive and controlling behaviour offences

2.156 In our draft section on other harassment offences, we did not provide substantive guidance on the priority offence of stalking. We noted that, while all offences related to stalking, harassment and coercive behaviour are very serious, "for the purposes of the ICJG, the sensible way to approach these offences is not necessarily to consider the most serious offence first." We reasoned that it was not likely to be straightforward for a service provider to identify specific instances of coercive and controlling behaviour (at least not consistently with the privacy rights of their users) because the provider would need to know whether the potential victim and perpetrator are or were in an intimate personal relationship, or are living together either as members of the same family. However, the coercive and controlling behaviour offence also requires the perpetrator to repeatedly or continuously engage in behaviour towards another person that is controlling or coercive, in a way that has a serious effect on them. A serious effect is where the victim fears at least twice that violence will be used against them, or is caused 'serious alarm or distress' which has a substantial adverse effect on the victim's usual day-to-day activities. The perpetrator is only guilty of the offence if they know or ought to know that the behaviour will have a serious effect on the victim.

2.157 We also noted that any case involving threats or abuse causing fear of violence, or alarm or distress, will be caught by the threats and abuse priority offences set out in paragraph 2.146. A case involving fear of violence, or alarm or distress which is not caught by those will be caught by the harassment offence in section 2 of the Harassment Act 1997 and/or Article 4 of the Protection from Harassment (Northern Ireland) Order 1997 (S.I. 1997/1180 (N.I. 9), which applies when a person engages in a course of conduct (a minimum of two instances, but these can include offline as well as online instances), which amounts to harassment of another, and which a reasonable person in possession of the same information would know or ought to know amounts to harassment. In other words, before a provider had sufficient information to make a reasonable inference of coercive and controlling behaviour, it would have already identified harassment and the takedown duty would already have been triggered. The same reasoning applies in relation to stalking and the racially or religiously aggravated harassment offences, since all involve harassment.

2.158 We therefore proposed to draft our ICJG with a focus on harassment. We reasoned that the other, more serious offences need not be considered in order to make an illegal content judgement, though they may well be relevant in considering the seriousness of the content and how it should be prioritised.

2.159 One stakeholder, [✂], argued that – while it is helpful to set a threshold for the takedown duty for harassment, it must also be noted that harassment, stalking and coercive and controlling behaviour are distinct offences set out in legislation, which should not be

conflated. The stakeholder noted that the police treat these offences as distinct as such when dealing with perpetrators and supporting victims.[63]

2.160 We have decided to go ahead with the same approach as proposed in the draft ICJG, focusing on harassment as we believe it remains the most practical and proportionate approach to multiple overlapping offences. However, we acknowledge the point raised by the stakeholder. We have therefore decided to add the following drafting to our guidance: "For the purposes of determining the illegality of content, harassment is the easiest to identify of a range of related and potentially serious offences, including stalking and controlling or coercive behaviour. However, as is set out in the Register of Risk, although related, these offences are distinct and can be perpetrated and experienced in many different ways." We have also added additional guidance on how service providers should approach risk assessments for other harassment offences, separating out risk assessments for stalking and CCB. This includes additional guidance on additional risk factors which may indicate CCB: where a particular users' account has been hacked, or attempted to be hacked, where a user is the target of multiple, unfounded or unsuccessful complaints, and where a user has been the victim of an intimate image abuse offence.

Inclusion of detailed guidance on stalking

2.161 The **Domestic Abuse Commissioner** expressed concern that our draft guidance said too little about stalking and did not acknowledge its interactions with the intimate image abuse offence.[64] We recognise the concern raised. In our final guidance, we have flagged that content raising concerns about threats, abuse and harassment (including hate) may also raise concerns about a number of other types of offence including adult image-based offences. We have emphasised that intimate image abuse is one of the adult image-based offences which may be particularly relevant.

2.162 We also acknowledge that it is important that victims' experiences of stalking are recognised as something distinct and distinctly harmful, and we are committed to encouraging service providers to manage the risk of harassment content as a discrete harm which has a separate profile and impact to other points of harassment. This is evidenced in our various pieces of guidance on risk assessment and management. Stalking as a harm and an offence is driven by repetitive behaviour rather than by single pieces of content, and so an approach which focuses on harm prevention and user empowerment may be most appropriate when managing this risk.

2.163 The ICJG, however, is about identifying "illegal content". As a type of content, in our view stalking is one of the kinds of harassment content. The harm caused by harassment and stalking can be different and different people may be mostly affected, but that is a matter for the risk assessment more than for the ICJG.

2.164 Similarly, when considering specific items of potentially illegal content for the purposes of the takedown duty, it does not matter whether content is illegal under one offence or multiple. The end result is the same: the content must be removed. As set out in the consultation to support the draft text, the offence of stalking necessarily includes harassment and therefore any illegal content which amounts to a stalking offence also, by definition, amounts to a harassment offence. Of the two, the harassment offence has the 'lower bar' and so we steered providers to consider this first as it encompasses the stalking

[63] [✂].

[64] The Domestic Abuse Commissioner's response to November 2023 Illegal Harms Consultation, p. 6.

offence and would capture stalking content alongside harassment content with no stalking element. Due to the quantity and complexity of the offences being considered, we prioritised ensuring that providers were able to make timely and accurate judgements that resulted in illegal content being removed swiftly.

Guidance on inchoate offences as they relate to coercive and controlling behaviour and domestic abuse

2.165 In the draft ICJG, we did not provide any substantive guidance on the coercive and controlling behaviour offence as any content amounting to this offence would already amount to a harassment offence, and we want to prioritise ease of use in cases where content could amount to multiple offences at the same time. **Refuge** called for further consideration of the inchoate versions of offences relating to coercive and controlling behaviour (CCB) and domestic abuse.[65] Specifically, it asked for consideration of whether guidance is required to outline where content may amount to an offence of encouraging an offence related to domestic abuse (for example, CCB, assault or grievous bodily harm).[66]

2.166 We have added more information about offences of encouraging, assisting and conspiracy to commit the offences in this section. Our final guidance gives, as an example of where content is likely to be illegal because it encourages or assists the commission of an offence, content consisting of instructional information about, or encouragement of, intimate partner surveillance, such as monitoring an intimate partner's electronic communications or movements. This is likely to amount to an offence of encouraging and/or assisting the commission of a harassment, stalking, or controlling or coercive behaviour offence. We considered it would be more difficult to infer intent in relation to assault or grievous bodily harm, though we are open to reviewing this if appropriate in future.

Child sexual exploitation and abuse (CSEA): Offences relating to child sexual abuse material (CSAM)

2.167 The Act defines a number of priority offences which relate to indecent or prohibited images of a child, defined as anyone under the age of 18 years old. The offences in question include making, taking, distributing, showing or possessing this kind of material.

'Possession', 'making' etc.

2.168 The prohibited image offence is committed by possession only. In the November 2023 Consultation we proposed that for the purposes of service providers making illegal content judgements, there is no need to consider the verbs used in the offences in detail. We said that if an indecent picture is available on the internet, it has been 'made'. If a prohibited image is available on the internet, it is 'possessed' by at least the user who uploaded it. We received no responses on this proposal and have therefore decided to go ahead with it as set out in our draft ICJG.

2.169 Similarly, we proposed that out draft ICJG would direct providers to consider the English, Welsh and Northern Irish offences. This is because we considered the comparative offences across the nations and noted that the Scottish version of the 'making' offence includes additional defences relating to what was reasonably believed by the person 'making' the image in respect of the child's age. The England, Wales and Northern Ireland offences do not include this, and are applicable to illegal content regardless of which part of the UK.

---

[65] Refuge response to November 2023 Illegal Harms Consultation, p. 25.
[66] Refuge response to November 2023 Consultation, p. 25.

Again, we have decided to go forward on this basis having received no responses on this matter.

Inferring the age of a subject in a potentially indecent image

2.170 An indecent image is any photograph or pseudo-photographic image or video of a person under the age of 18 which is "indecent by reference to recognised standards of propriety." When making inferences about the legality of potentially indecent images, inferences about the age of the subject of the image is therefore determinative of illegality.

Inferring the age of the subject from contextual information within the image itself

2.171 The draft ICJG stated that "when inferring the age of the child depicted in the content, service providers should make a common-sense judgement as to whether the subject of the image is under 18, using the general appearance of the subject and any contextual factors." In its response, **Yoti** expressed "reservations" about this proposal without providing any further detail.[67] Although it is unclear what the reservations concern, we have reviewed our drafting and believe that this approach is in line with what is practical for providers and reflects the high level of harm inherent in the posting of child sexual abuse material (CSAM).

2.172 In our November 2023 Consultation, we said that the age of a subject in an image should be inferred based on the general appearance of the subject(s) in the content itself and any contextual information that is available. We said that: "Such contextual information may include captions to the image or comments." In its response, the **Canadian Centre for Child Protection (C3P)** argued contextual information relevant to inferring age should also include settings within the imagery (e.g. appearance of a child's bedroom in background of the image/video).[68] It suggested that, as part of informal engagement, we should engage with relevant stakeholders to explore whether this approach this aligns with current practice and what evidence there is to show that contextual information enhances inference of age. We are open to exploring this approach further with relevant stakeholders at a later date, but believe it is also appropriate to make a small change to the ICJG now. We have decided to amend the relevant text to refer to "other relevant indicators within the image itself." In doing so we have purposefully avoided specifying unduly (for example, by referring to a child's bedroom in an image) so as to avoid the suggestion, which at present we are not in a position to evidence, that such indicators are determinative.

Inferring age from flags and reports from users other than the subject of the image

2.173 The draft ICJG stated that reasonable grounds to infer that the subject of the image is under 18 may exist in three circumstances, one of which was that "the subject of the image itself states in a report or complaint that they are aged under 18 or were aged under 18 at the time when the potentially illegal content was posted." The **Canadian Centre for Child Protection (C3P)** noted that this approach relies heavily on youth reporting situations, and that it does not consider situations where a parent/guardian, friend, or other person in a victim's life may provide information to the platform.[69] We are grateful for this comment, and have updated the ICJG to address it. The list of scenarios in which reasonable grounds to infer that the subject of the image is under 18 may exist now includes the following: "A person other than the subject of the image itself states in a report or complaint that they

[67] Yoti response to November 2023 Consultation, p. 25.
[68] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.
[69] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.

are aged under 18 or were aged under 18 at the time when the potentially illegal content was posted; and none of the factors mentioned at a) or b) suggest that the user is over 18."

Use of phrase 'good evidence'

2.174 In the November 2023 Consultation chapter accompanying the draft ICJG, we said that content need not be taken down if a service provider "had good evidence that a person who looked underage was in fact over 18" but that 'in the absence of good evidence we consider it reasonable for [service providers] to infer.' The **Canadian Centre for Child Protection (C3P)** called for more clarity on what constitutes 'good evidence,' suggesting that the term should have 'some parameters.'[70] We note that this phrasing does not appear in our final Guidance, except in new drafting where it is clearly explained what 'good evidence' means. For avoidance of doubt, 'good evidence' of a person being over 18 could be provided by age estimation or verification ('age assurance') or by a statement from the subject of the image themselves that they were over 18 at the time of the image being posted. Whilst we acknowledge that age estimation and self-declaration are not guaranteed ways to ascertain age, we believe that – in this particular circumstance – they would shift the balance of presumption, making it more reasonable to infer that a person *is* over 18 rather than that they were under 18. However, in absence of such evidence, as stated in the ICJG, subjects of images who *appear* under 18 should be assumed to *be* under 18 and content should be removed. If in doubt, providers should assume that the subject is underage and take down, deindex or downrank the content. We have made this clear in an additional piece of drafting which we have decided to add to the opening section of the CSAM chapter.

Inferring age from coded information on profiles

2.175 In their response, the **Canadian Centre for Child Protection (C3P)** drew attention to cases where child users share their age in their profile in a way which is coded or disguised, so it can be understood by those who recognise the techniques, but is less likely to be picked up by moderators.[71] They give the example of images with hidden numbers and maths problems in textual profile information. While we welcome this expert evidence, we believe it is unreasonable and disproportionate to expect service providers to actively seek out coded or hidden indications of age in a profile, except where these are well established or relatively obvious. To do so would risk the removal of non-illegal content posted by users who have inadvertently used the same or who have included numbers in their images for other reasons.

Use of/reference to age estimation technology

2.176 Age estimation technologies are software algorithms which make a statistical estimation of age based on the appearance of their face. In our November 2023 Consultation chapter, we explained that Ofcom is working to gather evidence regarding the use of age estimation and verification technologies and, after this work is complete, "many [service providers] will be expected to use age estimation or verification measures that are highly effective at determining whether or not a particular user is a child or not. This may make it easier for services to identify potential victims whom it is reasonable to infer are children." In its response, the **Canadian Centre for Child Protection (C3P)** raised concerns about this, highlighting evidence that such technologies can be inaccurate and arguing that there are

[70] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.
[71] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.

"bias/gaps with age estimation tools leaving users with false security."[72] We also said that service providers should have regard to the privacy implications of reviewing a potential victim's account activity and information in order to determine their age. The **ICO** called for further clarity as to whether reference to account information is intended to include the use of data derived from age assurance technologies.[73] It highlighted a potential contradiction between our consultation document and the CSAM chapter, and questioned whether account activity in general should be considered reasonably available information.[74]

2.177 In response we emphasise that we are *not* requiring age estimation/verification tools to be relied upon in the ICJG, although we are steering providers to take these into account where they are already available to providers. We accept that there are privacy and accuracy concerns in relation to these technologies, but we believe that it would be unacceptably risky to steer service providers *not* to take account of such information if it is available to them. The priority is to protect children from the creation and sharing of CSAM, although this should of course be done in a way which complies with data protection law.

2.178 In relation to account activity and information more generally, we can clarify that only account information in the form of statements of age is considered reasonably available. We believe that steering service providers to consider account activity when assessing the age of a potential victim would constitute a potentially very significant risk to privacy. For further clarity we have therefore removed reference to account activity from our guidance chapter altogether.

Further guidance on age estimation and training of moderators

2.179 Due to the focus on content judgements, the draft ICJG does not contain further recommendations about how moderators should be trained, including in the matter of estimating age. In its response, the **Canadian Centre for Child Protection (C3P)** noted that "what a reasonable person assumes is someone under 18 based on appearance is very open to interpretation" and that, as a result, "context/training of those reviewing/moderating the content can influence what they believe is reasonable."[75] We acknowledge the issues raised in this response, but believe our approach is the most appropriate at this time as we are not in a position at this stage to recommend specific training for identifying children through contextual clues. We believe our Codes set out proportionate recommendations on training, and the ICJG is not the place to do this. However, we are committed to continually monitoring our reviewing the ICJG and accompanying Codes measures (for example, requirements to have suitably trained staff) as more evidence becomes available to us.

Manga drawings and prohibited images

2.180 It is a priority offence under the Act to possess a prohibited image of a child. A prohibited image is a non-photographic or non-pseudo-photographic image which meets certain criteria set out in 4.38 of our final CSAM chapter. In our draft ICJG we set out that "examples of such images include cartoons or manga images, drawings, and CGI-generated images that are not lifelike in character."

---

[72] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.
[73] ICO response to November 2023 Consultation, pp. 25-26.
[74] ICO response to November 2023 Consultation, p. 24.
[75] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 32.

2.181 In its response, the **Wikimedia Foundation** expressed concern that current wording in the draft CSAM chapter could mean that "even linking to Wikipedia articles could be problematic," giving as an example the case of a Wikipedia article on 'Lolicon'.[76] Lolicon is a type of manga which depicts children in a sexualised and explicit manner. **Wikimedia Foundation** argued that such content is not illegal because it is not covered by the Protection of Children Act 1978 as it is neither a photograph nor a pseudo-photograph.[77] While it is correct that manga drawings are not covered by the 'indecent imagery' offence from the Protection of Children Act, it is incorrect that this means they are not illegal. Section 62 of the Coroners and Justice Act 2009 – possession of a *prohibited* image of a child – is a priority offence under the Online Safety Act. A prohibited image is a non-photographic or pseudo-photographic image which meets several criteria as outlined in our final ICJG at 4.38 and can include drawn depictions such as manga. Our ICJG is thus reflective of the law and no changes have been made.

Inclusion of hyperlinks

2.182 The **Wikimedia Foundation** also expressed concern about our proposed approach to hyperlinking.[78] In our draft ICJG, we stated that "if the content concerned is a link to an indecent or prohibited image of a child or a paedophile manual… services will have reasonable grounds to infer that this amounts to a priority offence." We considered it particularly important to make this clear for the following reasons:

a) Under section 7(4) of the Protection of Children Act 1978, reference to a photograph includes data stored by electronic means which is capable of conversion into a photograph.
b) It is reasonable in any event for a service to infer that a person sharing a URL of that nature knows what it leads to and intends the person with whom they share it to click on.
c) Dissemination of URLs is likely to amount to distribution or showing of indecent images as the case may be.
d) The definition of 'publish' for the purposes of section 2 of the Obscene Publications Act 1959, in relation to obscene publications, includes 'distribute' (see section 1 of that Act)

2.183 In its response, **Wikimedia Foundation** stated that "The cumulative effect of Ofcom's proposed Guidance is to require platforms to treat any member of the public as distributing CSAM if they post a URL to a [Wikipedia page such as the 'Lolicon' article, which contains potentially illegal content involving a prohibited image of a child] or others like it."[79] Specifically, it suggested that Ofcom are 'creating a stringent interpretation of UK law regarding hyperlinking" and questioned the implication that accessing a copy of a Wikipedia article which contains a prohibited image of a child would amount to 'making' CSAM.[80]

2.184 We confirm that this is indeed the intended effect of the ICJG, where the content at the URL posted contains a prohibited image such as a pornographic drawing of a child which is obscene (or grossly offensive or disgusting). Such content is illegal content and therefore hyperlinks to this content should be treated as equivalent to the posting of the content itself, as set out in the ICJG. The legal definition of 'making' an image includes accessing an

[76] Wikimedia Foundation response to November 2023 Illegal Harms Consultation, p. 40.
[77] Wikimedia Foundation response to November 2023 Consultation, p. 40.
[78] Wikimedia Foundation response to November 2023 Consultation, p. 40.
[79] Wikimedia Foundation response to November 2023 Consultation, p. 41.
[80] Wikimedia Foundation response to November 2023 Consultation, p. 41.

image in this context, and so there would be reasonable grounds to infer that anyone accessing an image via such an article has 'made' the image in the legal sense of the word. As a result of this, we have made no changes to the ICJG.

Language

2.185 The **Centre of Expertise on Child Sexual Abuse** made a couple of points regarding language used in the ICJG's CSAM chapter. Firstly, it argued that acronyms like 'CSA' should be avoided.[81] We accept that the use of acronyms is not always ideal but believe it is warranted in some cases, where the acronyms are well-established, promote rather than reduce readability, and they have been defined for readers. We believe this to be the case in the examples of child sexual exploitation and abuse (CSEA) and child sexual abuse material (CSAM) as they are well established acronyms the use of which promotes readability by reducing the 'wordiness' of a sentence. Secondly, it argued that the term 'child sexual abuse' covers a range of behaviours that take place within a wide range of different contexts and that individuals often have different understandings of this term. It argued that it can therefore be helpful to victims and survivors to hear the different contexts of child sexual abuse mentioned to help them feel recognised. We recognise this point and have decided to update our guidance to include a broad definition of child sexual abuse taken from the Independent Inquiry into Child Sexual Abuse. We believe this is an appropriate level of detail given the specific focus of the ICJG (helping service providers make content judgements). However, it should be noted that only CSAM and grooming offences are captured by the Act and therefore the ICJG.

Child sexual exploitation and abuse (CSEA) - Grooming and exploitation of children

2.186 The remaining CSEA offences relate to behavioural sexual exploitation and abuse of children in the form of 'grooming'. There are a number of priority offences relating to the grooming which can be grouped into the following categories:

a) sexual activity offences in which the potential victim is under 16;
b) adult to child offences in which the potential victim is under 16;
c) 'arranging' together with 'assisting', 'encouraging' and 'conspiring' offences which could take place between adults and/or children, and in which the potential victim or victims are under 16; and
d) offences concerning the sexual exploitation of children and young people aged 17 and younger.

2.187 We did not receive any challenge from stakeholders in response to our November 2023 Consultation on some of our proposals, and we have not changed them. Apart from the changes we described at the beginning of this chapter, our final guidance, and our reasoning for it, therefore remains the same as at consultation. We set out that reasoning in the annex titled 'Annex to Volume 3'. This relates to the offences on meeting a child following sexual grooming or preliminary contact, and the sexual exploitation of a child offences.

Threshold for suspected illegal content

2.188 Commenting broadly on our chapter on grooming, the **NSPCC (National Society for the Prevention of Cruelty to Children)** argued that the ICJG should state that service providers

[81] Centre of Expertise on Child Sexual Abuse response to November 2023 Consultation, p. 7.

can and should act on content where they have 'reasonable suspicion' that content or activity is illegal.[82] In response, we note that the ICJG is concerned with illegal content, which is defined by a threshold of 'reasonable grounds to infer' that the content amounts to a relevant offence. This threshold is what providers should act on. In relation to potential grooming content, the bar for what 'reasonable grounds to infer' may consist of is relatively low (see paragraph 5.3 of the ICJG). As set out in our introduction, service providers are also free to act on content above and beyond what is illegal under the Act, so long as they do so in compliance with their other duties.

Sexual communication with a child in immersive environments

2.189 In its response, the **NSPCC (National Society for the Prevention of Cruelty to Children)** also drew attention to the threat of virtual reality spaces providing opportunities for child sexual abuse and exploitation. It made the point that judging whether content is illegal in these types of online spaces will be complex and differ from other online spaces.[83] The **NSPCC (National Society for the Prevention of Cruelty to Children)** also suggested that reasonably available information might be different in these spaces, particularly because of the different way in which service providers record audio and video interactions in immersive environments.[84] It recommended that Ofcom set out how illegal activity should be identified and judged in immersive environments, including through the use of usage examples, and on how information should be stored in a safe and privacy-preserving manner to help service providers identify and report illegal content.

2.190 We recognise the particular risk of child sexual abuse and exploitation in immersive environments where content created is ephemeral and therefore difficult to moderate. Our ICJG introduction chapter explains that illegal content can be written messages, audio, video and images of any kind. Whether the content is ephemeral or not, and whether it originates in an immersive environment or not, is not relevant to a content judgement. However, we recognise the point that the **NSPCC (National Society for the Prevention of Cruelty to Children)** make regarding the particular risk that exists in relation to immersive environments, and have therefore decided to add additional drafting to the final ICJG chapter on the grooming offences. The additional drafting states that illegal content will be illegal regardless of the environment in which it is posted (including in virtual reality and other immersive environments).

Inferring the age of a potential victim of grooming

2.191 As noted in paragraph 2.187, the age of the potential victim is central to establishing whether a grooming offence has occurred. It is therefore necessary for service providers to make reasonable inferences about whether a potential victim is under 16, or aged 17 or under in the case of sexual exploitation offences.

2.192 Where content concerns the grooming and exploitation of children offences, there may not be an image, or at least not a current one, which the service provider can necessarily use as the basis for drawing inferences about age.

2.193 Our November 2023 Consultation chapter noted that, in future, service providers will be expected to use highly effective age estimation or verification measures and that this will likely make it easier to identify potential victims whom it is reasonable to infer are children.

---

[82] NSPCC response to November 2023 Illegal Harms Consultation, pp. 50-51.
[83] NSPCC response to November 2023 Consultation, p. 50.
[84] NSPCC response to November 2023 Consultation, p. 51.

We included "robust age estimation or age verification measures indicate that the potential victim is aged under 16" as one of the indicators that would provide reasonable grounds to infer that a potential victim is a child. In its response, **Yoti** expressed "reservations" about our approach, without providing further detail.[85] We have thus revisited our drafting to look for areas of improvement, but judge that our drafting strikes the correct balance at this time, as we are not able to compel the use of age assurance technologies without further work and evidence.

2.194 Generally speaking, in our view, self-declaration is not a good way to infer age. This is partly because children may declare themselves to be over 18 in order to access age-restricted content, and partly because would-be abusers may declare themselves to be children in order to gain access to children. However, for the specific purposes of making illegal content judgements about grooming, our view is that a potential victim of grooming, who declares themselves to be a child, should usually be believed. This is because:

a) many children do give their age truthfully;
b) abusive adults who claim to be children are unlikely to make complaints about grooming; and
c) although there is some risk of malicious reporting, the content itself would need to meet the definition of the offence, which would be relatively difficult for malicious reporters to achieve.

2.195 Service providers should therefore use information where a potential victim states their age (for instance in the relevant content itself or in other places associated with the potential victim's account) as a way to infer their age.

2.196 We do not consider that the same can be said of potential perpetrators. Our view is therefore that reasonable grounds to infer that a perpetrator is 18 or over may arise in any of the following ways:

a) The potential perpetrator states they are aged 18 or over;
b) The potential perpetrator has been using the service for 18 years or more;
c) The potential victim provides evidence that the potential perpetrator is aged 18 or over, and the service provider is not aware of any strong evidence to suggest the contrary.

2.197 The draft ICJG chapter on grooming stated that reasonable grounds to infer that the potential victim of grooming is under 16 may exist in three circumstances, one of which was that "the subject of the image itself states in a report or complaint that they are aged under 16 or were aged under 16 at the time when the potentially illegal content was posted." The **Canadian Centre for Child Protection (C3P**) noted that this approach relies heavily on youth reporting situations, and that it does not consider situations where a parent/guardian, friend, or other person in a victim's life may provide information to the platform.[86] We welcome our attention being drawn to this omission and have updated the ICJG to address it.

2.198 The **Canadian Centre for Child Protection (C3P)** stated that "the context of discovery of the situation may assist with the determination of when the service provider can reasonably infer what a potential victim is under 16."[87] Examples included in its response were if someone reported content to the provider or if the provider detected the content using

[85] Yoti response to November 2023 Consultation, p. 25.
[86] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 33.
[87] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 33.

their own moderation tools. It argued that this contextual information could for instance be whether a report was made by a friend, a parent/guardian or an agency, NGO, or other reporting entity.

2.199 We agree that if a report has been made about a piece of content, information included in this report should be considered by a service provider. This is reflected in the boxes summarising reasonably available info set out in the ICJG chapter. Regarding reports from agencies, NGOs and other reporting entities, we recognise this point and have decided to add reports from law enforcement or other specialist agencies (such as the NSPCC) to the list of reasonably available information that should be taken into account when making judgements about potential grooming content. Finally, we agree that if, in theory, a report was made by a friend or parent/guardian of a potential victim of grooming, this might help providers establish whether a potential victim is under the age of 16. However, service providers are unlikely to have a way to verify if a user report has actually been made by a friend or parent/guardian as users can easily say they are someone's friend or parent/guardian when this is actually not true. We have therefore decided not to set out in the ICJG that providers should have particular regard to a report if it was created by someone claiming to be the potential victim's friend or parent/guardian.

2.200 Reflecting on our response to the **Canadian Centre for Child Protection's (C3P)** points, we have expanded the list of scenarios in which reasonable grounds to infer that the subject of the image is under 16 may exist. It now includes the following: "A person other than the potential victim of grooming states in a report or complaint that the potential victim is aged under 16 or was aged under 16 at the time when the potentially illegal content was posted", unless:

i) Information from age estimation or age verification measures ('age assurance measures') indicate that the potential victim is aged 16 or over; or
ii) The potential victim stated in a report or complaint that they were aged 16 or over at the time the potentially illegal content was posted.

Use of/reference to age estimation technologies and account activity

2.201 In our November 2023 Consultation chapter, we explained that Ofcom is working to gather evidence regarding the use of age estimation and verification technologies and, after this work is complete, "many [service providers] will be expected to use age estimation or verification measures that are highly effective at determining whether or not a particular user is a child or not. This may make it easier for [providers] to identify potential victims whom it is reasonable to infer are children." We also said that service providers should have regard to the privacy implications of reviewing a potential victim's account activity and information in order to determine their age. In its response, **ICO** called for further clarity as to whether that reference to account information is intended to include the use of data derived from age assurance technologies.[88] Further, the **ICO** highlighted a potential contradiction between our consultation document and the grooming chapter, and questioned whether account activity in general should be considered reasonably available information.

2.202 In response we emphasise that we are not requiring age estimation/verification tools to be relied upon in the ICJG, although we are encouraging service providers to take these into account where they are already available to providers. While there may be privacy and

[88] ICO response to November 2023 Consultation, pp. 25-26.

accuracy concerns in relation to these technologies, we believe that it is proportionate for service providers to take account of such information if it is available to them, in the context of protecting children from the harm of online grooming. We have, however, reminded service providers that this should be done in a way which complies with data protection law and included a link to ICO's opinion on age assurance.

2.203 In relation to account activity and information more generally, we can clarify that only account information in the form of statements of age is considered reasonably available. We believe that steering service providers to consider account activity when assessing the age of a potential victim would constitute a potentially very significant risk to privacy. For further clarity we have therefore removed reference to account activity from our guidance chapter altogether.

Children representing themselves as over 16 online

2.204 Several of the offences which deal with sexual activity with a child break the offences down depending on whether the child is under 13, or whether they are between 13 and 15 years old. The main difference between the offences is the severity of the potential penalty. This is not, however, relevant to the question of whether the content is illegal content. We therefore proposed to deal with both groups of offences as content relating to potential victims under the age of 16.

2.205 However, for some offences, such as the offence of causing or inciting a child to engage in sexual activity, there is an additional element to be considered where the child is aged 13, 14 or 15, which is not required where the child is under 13. That is, for content to be considered illegal content, there must be reasonable grounds to infer that the potential perpetrator did not reasonably believe that the child in question was 16 or over.

2.206 When deciding our proposed approach to this discrepancy, we considered that our guidance will be in place at a time when some providers may not yet have robust age verification or age assurance measures in place enabling them to determine whether a child is under 13, or is 13, 14 or 15 years old. As a result, we proposed that, where providers are able to reasonably infer that a potential victim is under 16, this provides reasonable grounds to infer that the potential victim is not generally seeking to represent themselves to others as being over the age of 16. In these cases, service provides can infer that the potential perpetrator did not reasonably believe the child in question was 16 or over, and we proposed that the content should be treated as illegal and taken down, *except* where the victim has a made a positive statement that they have represented themselves to the other user as being aged 16 or over. The **Canadian Centre for Child Protection (C3P)** raised concerns about this in their response, stating that children who represent themselves as over 16 or 18 may be particularly vulnerable.[89]

2.207 We recognise this concern and other concerns raised regarding how service providers can go about inferring the age of a potential victim or survivor of child sexual abuse. A self-declaration from a user stating they are over the age of 16 is to be considered alongside other indicators that a user might be under the age of 16, such as age estimation or age verification measures ('age assurance measures') and should not on its own be considered determinative. However, if a provider is still in doubt, they are encouraged to remove the

[89] Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 33.

content in the interest of the safety of a potential victim of grooming. We have added wording to this effect to paragraph 5.3.

Language

2.208 The **Centre of Expertise on Child Sexual Abuse** made a point regarding language used in the draft ICJG to describe child sexual exploitation and abuse offences, arguing that the focus should be "on the behaviour rather than the person."[90] As part of this, it suggested that the word 'perpetrator' should be avoided, especially in relation to children, and be replaced with 'the one who sexually abuses'. We recognise and accept that the language used to describe these difficult issues must be sufficiently sensitive, but believe that the use of 'potential perpetrator' in relation to adults who are posting content which may amount to a grooming offence is appropriate. However, we fully accept the importance of not representing children as perpetrator and have revisited our chapter to ensure that, where a child is able to commit a grooming offence, the language we used refers to 'other party'. We have chosen this more neutral language in recognition of the fact that the threshold is not criminal and therefore it cannot be said beyond reasonable doubt that the person has sexually abused.

Fraud and other financial offences

2.209 The priority fraud and other financial offences are listed in schedule 7 of the Act. They broadly comprise:

a) False claims to be authorised or exempt for the purposes of carrying on regulated activity (the first of the financial services offences);
b) Fraud by false representation;
c) Fraud by abuse of position and participating in fraudulent businesses carried on by a sole trader;
d) Other financial services offences;
e) Fraud related to misleading statements or impressions about investments;
f) Offences related to articles for use in fraud; and
g) Offences related to criminal property.

2.210 In this section we discuss offences on which we received more substantive responses: false claims to be authorised or exempt for the purposes of carrying on regulated activity, fraud by false representation and offences related to criminal property. A summary of our decisions regarding offences c) through f) in the list at paragraph 2.210 can be found in the annex titled 'Annex to Volume 3'.

Trusted flaggers

2.211 Ofcom's Illegal Content Code of Practice for other duties recommends that providers establish and maintain a separate reporting channel for the use of trusted flaggers. The measure states that, at minimum, trusted flagger status should be available to a number of entities, all of which have competence, expertise and knowledge in detecting and investigating one or more of the offences set out in the ICJG chapter on 'Fraud and other financial offences.'

2.212 In light of this, we have decided to add a section on trusted flaggers into the front our fraud chapter which sets out the entities which are specifically recommended to be trusted flaggers under the Code. This section replaces the similar, though more limited, section on

[90] Centre of Expertise on Child Sexual Abuse response to November 2023 Consultation, p. 7.

'Financial services offences' in the draft guidance on which we consulted. We consider that trusted flaggers are relevant to all offences, not just the financial services offences.

2.213 We have also decided to expand the previous section to state clearly the limits of the role of trusted flaggers. We now state that "Providers should take seriously any report from a trusted flagger within its area of expertise," noting that they are "entitled to assume that any evidence and information provided with such a report is true so far as the entity concerned is aware, and that reasonable enquiries have been carried out". This is due to the highly technical and complex nature of the fraud and financial services offences. However, we are aware that trusted flaggers should not, in all cases, have the power to trigger automatic takedown and believe it is necessary to make this clear to protect freedom of expression. As such, we have also decided to state that "Except in the limited circumstances [related to offences from the Financial Services and Markets Act 2000]… a provider is not required to accept the opinions of such a third party as to whether content is illegal content."

2.214 We remain of the view that the financial services offences are so complex and technical that it is not reasonable to expect that service providers will be able to apply them correctly. Nor can we summarise them in a way which reduces their complexity, as this would almost certainly result in Ofcom misleading service providers and the public about the offences. We do not think we can proportionally ask providers to take down all content which appears to promote investments. But we consider that significant harm would continue if we give guidance that a service provider is not expected to identify any financial services offences content as illegal content.

2.215 We therefore set out, in relation to the more complicated financial services offences, that we consider it appropriate for service providers to rely on the opinion of the FCA and PRA. We recognise that this means services are likely to rely on those bodies' judgment heavily, with possible unfairness to users and risks to their commercial interests and to their rights to freedom of expression. We gave particularly anxious consideration to the freedom of expression implications of this guidance.

2.216 However, having considered all the competing rights concerned, in particular the significant harm arising out of misconduct in this regulated area and the rights of internet users to be protected from crime, we consider the impact on the right to freedom of expression to be proportionate. The FCA and PRA are public bodies bound their own duties not to act unfairly or incompatibly with the right to freedom of expression. They have significant technical expertise and experience and are far more capable than service providers are of making decisions which are correct. The offences concerned relate to financial services. Our guidance therefore does not appear at all likely to impact on the most highly protected forms of speech such as political speech, religious speech or creative speech. Overall, we consider this the best way to balance the competing interests of users and service providers.

Fraud by false representation

2.217 It is an offence to 'dishonestly make a false representation' where the person making such a representation intends to make a gain thereby (for themselves or others) or to cause another person loss (or expose them to the risk of loss). In our draft ICJG we said that content should be considered illegal where "there are reasonable grounds to infer that it contains a false representation… that was made dishonestly for either of these two

purposes. In order for content to be considered illegal, services do not need to infer that the representation resulted in an actual gain or loss."

Indicator list – overall approach

2.218 As acknowledged at consultation, the offence of fraud by false representation is undeniably complex. For content to amount to this offence, a provider would need reasonable grounds to infer that it contains a statement which is false, that it is dishonest, and that the user intends to make a gain or cause a loss. All these things are matters which involve drawing inferences about circumstances offline. For a statement to be false, there must be a 'truth' which exists outside the content. Dishonesty and intent are both parts of the user's state of mind.

2.219 Recognising the difficulty of these judgements, we proposed that it *is* possible to draw reasonable inferences in some circumstances, based on the content and the context in which it appears. This is likely to be the case for the most egregious examples of this type of content. We therefore proposed to use a 'filter system' to identify content which may reasonably be inferred to amount to fraud by false representation. This was because whilst certain features of online content might raise concerns about fraud by false representation, it would be unusual for a single representation to provide on the face of it reasonable grounds to infer that it is false; that it is dishonest; and that the user intends to make a gain or cause a loss.

2.220 The filter system we proposed contained a non-exhaustive list of suggested 'red flag indicators', split into three categories:

a) Disguised account information or activity. For example, a user masking their location;
b) Requests, invitations or inducements to invest, send money, send identification documents, or send financial information. For example, a user asking another user to send money, ID documents, bank details, personal information or contact information.
c) Account and content characteristics commonly associated with fraudulent behaviour. For example, the use of apparently misspelt words, or users registering multiple or repeat accounts that share the same phone number, IP address/device identifier, password or date of birth (except where there appears to be a legitimate reason to do so).

The first category 'and third categories focused on identifying features of that content which might point to dishonest intention, and might in context amount to reasonable grounds to infer that the representation being made is false (if not apparent on the face of the content). The second category filtered by content which contains a relevant 'representation'. Without a representation, which is made with the intention to make a gain or to cause another person loss (or expose them to the risk of loss), there can be no offence of fraud by false representation.

2.221 We emphasised in our November 2023 Consultation chapter that no single indicator will be a guarantee of fraud by false representation. It is only in cases where there is content of the type suggested in each category where may be reasonable grounds to infer fraud by false representation except where service providers have evidence to suggest the contrary. Whether or not there are reasonable grounds to infer fraud by false representation in relation to any piece of content, will ultimately rest with providers and will be a case-by-case decision.

2.222 A significant proportion of the responses relating to the fraud chapter concerned our proposed 'red flag indicator' groups system. Responses were broadly welcoming of the approach in principle. Stakeholders such as **Which?**, and the **Advertising Standards Authority** recommended additional red flag indicators, and **Lloyds Banking Group** urged Ofcom to regularly update these as they will quickly be out of date as bad actors change their mode of operating. [91] **UK Finance** argued that the list of indicators was not ambitious relative to criminals' aggression, noting that there is information available to service providers from sources such as the financial services sector.[92] **UK Finance** also argued that the steer that at least one indicator from Group 1 *must* be present for content to amount to fraud by false representation will "leave gaps."[93]

2.223 We acknowledge that our proposed approach risked becoming quickly out of date and risked missing out information that is available to service providers from sources besides Ofcom. We welcome the evidence provided regarding the financial services sectors' use of multiple tools to understand risk signals.[94] In our final guidance, we have taken an approach of setting out what needs to be shown, for content to amount to the offence, and using our 'red flag indicators' to illustrate rather than exhaustively define when reasonable grounds to infer that content is illegal may arise.

2.224 Our Guidance now states that: "In the guidance below we have provided illustrative examples of 'red flag indicators' to assist service providers to identify content amounting to an offence of fraud by false representation. But these red flag indicators are not exhaustive. The main point to note is that in in order to identify fraud, services should not look for just one factor but instead look at a combination of factors. It is important to underline that the majority of the examples provided are not, in isolation, capable of constituting illegal content."

2.225 We have separated our original proposed 'red flag indicators' into four groups based on the necessary requirements of the fraud by false representation offence:

a) There must be some sort of a representation, which may relate to the identity of the user or to information within the content in question (or both);
b) There must be some information which suggests the representation is false;
c) There must be some information which could lead to a loss/gain; and
d) There must be some information which suggests that the user posting the content[95] is doing so dishonestly.

2.226 We remain of the view that it will often be reasonable to consider a red flag indicator as evidence of more than one of these requirements, but that no one indicator is sufficient on its own.

2.227 Under "Information which suggests the representation is false" we have added subcategories to help illustrate the types of reasonably available information that a service should consider. These subcategories include "content specific anomalies", "technical anomalies and unusual user behaviour", and "historic/current reports and complaints".

---

[91] Advertising Standards Authority response, 2023, pp. 7-9. Lloyds Banking Group response to November 2023 Consultation, p. 11. Which? response to November 2023 Illegal Harms Consultation, pp. 12-13.
[92] UK Finance response to November 2023 Consultation, p. 16.
[93] UK Finance response to November Consultation, p. 16.
[94] Lloyds Banking Group response to November 2023 Consultation, p. 11.
[95] An account name and information provided on a user's account profile is also content.

Indicator list – specific indicators

2.228 We have also looked carefully at the suggestions made by respondents and have decided to add the following indicators:

a) Links to a contact method (for example, a website, telephone number or email address) different from that brand or organisation's known official channels (under "information which suggests that the user posting the content is doing so dishonestly").
b) A claim that an investment or the firm concerned is regulated by a body which does not exist (This is a particularly serious example and is very likely to be associated with a fraud).
c) The use of 'non-printable characters' to evade detection (under "information which suggests that the user posting the content is doing so dishonestly").

2.229 We considered adding the following indicators but were concerned that they were too associated with non-fraudulent content:

a) Use of lifestyle accounts.
b) Sensationalist headlines about celebrities.
c) Edited or inauthentic images, AI generated images, and celebrity images, which can be clicked on through an embedded hyperlink (taking users off-site), or are used in conjunction with a link prompting users to move off site.

2.230 Instead, we have identified all these factors as matters which are often associated with fraud. While they do not necessarily provide grounds for a reasonable inference, they may (where the provider concerned is in a position to identify them) be helpful in identifying risks or prioritising content for review.

2.231 We also considered adding the following indicator: "A large proportion of reviews reporting that the offer is a scam, that they did not receive the product, or that it was not as advertised." However, we did not consider it proportionate to expect service providers to retrieve such information at scale.

2.232 In response to the point raised by **UK Finance** regarding the ambition of the ICJG, we recognise that there will be other relevant information which *may* be available to services when making judgements about fraudulent content. However, we believe that what is included in the ICJG is both relevant and *reasonably available* to platforms, as opposed to being available only to some platforms with existing relationships with experts.

The Advertising Standards Authority's Scam Ad Alert system, and influencer and paid-for advertising

2.233 In its response, the **Advertising Standards Authority** drew attention to its Scam Ad Alert system, a system in which for online paid-for fraudulent advertisements which are clear cut scams.[96] The ASA believes that this Scam Ad Alert system is likely to include some content which falls within the OS regime. It argued that it would be beneficial if Ofcom were to share more detailed guidance and definitions on content which is both within and outside of scope, particularly in relation to content which we consider to be advertising (including non-paid-for, paid-for and influencer), with specific examples where possible.

2.234 We have assessed the evidence provided about the Scam Ad Alert system. Our understanding is that the Scam Ad Alert system does not cover U2U, influencer-posted

[96] Advertising Standards Authority response to November 2023 Consultation, pp. 4-5.

advertising and we therefore believe it would be inappropriate to reference this in the ICJG specifically.

2.235 We can confirm that the fraud by false representation offence applies to all content as defined by the Act. Our position as set out in our November 2023 Consultation has not changed. The duties in relation to paid-for fraudulent advertisements are not yet in force, and we will update the ICJG as appropriate when we consult further on this issue. Influencer advertising is considered to be user-generated content and is therefore in scope of the regime and can be considered illegal content where it amounts to an offence of fraud by false representation. We have decided to add a definition of user-generated content to our Legal Annex which makes it clear that user-generated advertising (for example, influencer advertising or content posted by a brand or company to their own account) is in scope of user-generated content whereas paid-for advertising is not.

Approach to links used in content potentially amounting to fraud by false representation

2.236 As part of our indicator system, we indicated that content amounting false representation may involve invitations to send money, monetary instruments or digital assets, or to send other financial or identification information. In its submission, the **Advertising Standards Authority (ASA)** argued that much scam ad content uses the 'cloaking' technique, whereby users clicking through from links to products or services are directed to scam websites which seek to obtain their financial information or personal details.[97] It also drew attention to the growing frequency of ads which falsely claim to be from established retail brands, stating that "it is evident that the landing page [for such ads] is not for the claimed retailer." The **ASA** argued that "the content of the website an ad links to is a vital step in determining whether the ad itself is a scam or not" and suggested that we should consider whether the content of websites to which posts link, should also be referenced in the ICJG.[98]

2.237 We acknowledge the **ASA's** argument, but are concerned about the potential risks that could be posed to moderators and service providers more widely by the clicking of potentially fraudulent links. While we are aware that some service providers use URL checkers – tools which check URLs for the presence of malware, phishing attacks, botnets, and fraudulent websites – to test the safety of links which they may wish to follow, we are not in a position to recommend the use of such services when making content judgements, and so cannot ensure that such risks could be mitigated effectively. We have therefore decided to state that: "Where service providers are considering a piece of content which makes a representation which may be false and uses a URL link to do so, they should be aware that particular risks may be associated with accessing the link in question. Where service providers choose to follow links, it may be appropriate for them to use a URL checking service before doing so."

Offences relating to criminal property

2.238 At consultation, we took a descriptive approach to offences relating to criminal property, setting out the offences as they appear in law. We have not received new evidence or feedback that supports a difference in approach, so have broadly decided to maintain this at Statement. However, we have added an example of content which is likely to be illegal because of this offence: content offering stolen credentials for sale, where it is clear that they are stolen.

---

[97] Advertising Standards Authority response to November 2023 Consultation, p. 6.
[98] Advertising Standards Authority response to November 2023 Consultation, pp. 6-7, p. 8.

Drugs and psychoactive substances

2.239 In the draft ICJG, we provided guidance on the priority offences relating to controlled drugs, psychoactive substances and articles for the administering or preparing of controlled drugs. There were no major concerns raised by stakeholders in relation to our proposals in the chapter on drugs and psychoactive substances. We have therefore decided to publish this chapter of the ICJG largely unamended, with our major policy proposals remaining as they were at time of consultation. Our response to stakeholder responses in this area can be found in the annex titled 'Annex 1 to the statement on Further stakeholder responses', and our detailed reasoning can be found in the annex titled 'Annex to Volume 3'. In Annex 1 to the Statement on Further stakeholder responses we have also explained some other minor changes we have decided to make to the chapter.

2.240 We do, however, note a legislative change, as of November 2023, regarding nitrous oxide (also known as laughing gas). Under the Misuse of Drugs Act 1971 nitrous oxide is a Class C substance and it is illegal to possess, supply, import, export or produce nitrous oxide outside of its intended legitimate purposes. Our ICJG has been amended to reflect this recent change.

Weapons offences: firearms

2.241 The Act makes numerous offences relating to firearms priority offences. The offences in question broadly relate to the purchase, sale or transfer of firearms without the proper authority. In our approach to the very detailed and numerous offences, we tried to simplify the thought process for providers. We did not receive consultation responses on this approach. Our decisions in relation to the firearms offences are set out in full in the annex titled 'Annex to Volume 3'.

Guidance on deactivated weapons

2.242 **The Deactivated Weapons Association (DWA),** noted that, although it included information on replica and antique weapons, the draft Guidance provided no specific information on the legal status of firearms which have been deactivated to an official UK standard.[99]

2.243 We have addressed this in the final ICJG by making it clear that deactivated firearms can be legally bought, sold and (crucially, in this context) exposed for sale. Clear evidence that a firearm is deactivated, and thus not subject to the prohibitions outlined regarding exposure for sale, may come from either or both of the following pieces of reasonably available information:

a) the content states that the firearm being exposed for sale is deactivated; or
b) there is visual evidence, in the form of an appropriate mark from Proof House, that the firearm being exposed for sale has been deactivated.

Guidance on Violent Crime Reduction Act 2006 and realistic imitation firearms

2.244 As part of its response, one stakeholder [✂] drew attention to the lack of guidance on offences taken from the Violent Crime Reduction Act (2006).[100] This Act creates offences relating to the manufacture, sale or import of realistic imitation firearms (RIFs), as well as the conversion of imitation firearms into RIFs. We believe offences related to RIFs are adequately covered in paragraphs 8.97-8.101 of the ICJG, in which we outline how content may amount to an offence of encouraging or assisting a RIF to be imported into the UK. We

[99] Deactivated Weapons Association response to November 2023 Illegal Harms Consultation, 2023.
[100] [✂].

believe these are the most relevant and appropriate offences to consider, as there is no specific offence covering the exposure of RIFs for sale (that is, their advertisement for sale).

Weapons offences: knives and 'offensive' weapons

2.245 In addition to the offences on firearms, the Act designates certain offences related to knives and offensive weapons as priority offences. We provided guidance on the 'exposure for sale' elements of the sale of knives, crossbows and offensive weapons.

2.246 No major concerns were raised by stakeholders in relation to our proposals in the section on knives and offensive weapons. We have therefore decided to publish this chapter of the ICJG with our main policy proposals remaining as they were at the time of consultation. Our full reasoning is set out in the annex titled 'Annex to Volume 3'.

2.247 We note, however, that there have been changes to the law regarding the definition of zombie knives.[101] We have reflected these in our final Guidance. We are also aware of future plans by the government to review knife and weapon legislation, and will monitor this situation and update our guidance if appropriate. However, in order to ensure that our guidance is up to date, the ICJG includes a link to the government's webpage on 'Selling, buying and carrying knives and weapons', which contains a list of banned knives and weapons. This list will be kept up to date as legislation is changed, and we have decided to add drafting to our ICJG chapter on knives which "encourage[s] [service providers] to refresh their knowledge regularly as this list may change."

Sexual exploitation of adults

2.248 The sexual exploitation of adults offences comprise causing or inciting prostitution for gain[102] and controlling a prostitute for gain.[103]

Terminology

2.249 In the draft ICJG, we used the terms 'sex worker' and 'sex work' in sections discussing offences relating to the sexual exploitation of adults. We used the terms 'prostitute' and 'prostitution' only when referencing legislation that uses those words, using 'sex worker' and 'sex work' in other contexts. One stakeholder, [✂], criticised Ofcom's use of the terms 'sex worker' and 'sex work', while another stakeholder, **Changing Lives**, expressed support for us using this terminology.[104]

2.250 We recognise that 'sex worker' and 'sex work' are contested terms and that there are implications of using either those terms or 'prostitute'/'prostitution'. Ofcom took the approach of using 'sex worker' and 'sex work' predominantly because of concerns raised by stakeholders that some people and communities can feel stigmatised and upset by the use of the terms 'prostitute' and 'prostitution'. We understand that the broad consensus among representatives of people involved in this work is to use the terms 'sex worker' and 'sex work'. The National Police Chiefs' Council's 'Sex Work National Police Guidance' for instance states: "Language around prostitution is often perceived as outdated and pejorative among those selling sex. Use of 'prostitution' and its derivatives should be

[101] Criminal Justice Act 1988 (Offensive Weapons) (Amendment, Surrender and Compensation) Order 2024.
[102] Section 52 of the Sexual Offences Act 2003; article 62 Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2).
[103] Section 53 of the Sexual Offences Act 2003; article 63 Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2).
[104] Changing Lives response to November 2023 Illegal Harms Consultation, p. 16. [✂].

limited to specific legal meanings and offences." We have therefore decided to continue to use those terms in our final ICJG. However, we will continue to monitor this and review our approach if and when necessary.

Causing or inciting prostitution for gain

2.251 This offence requires the potential victim to be at risk of becoming a prostitute because of the action.[105] It is therefore implicit within the definition of the offence that the potential victim was not already involved in sex work prior to accessing the content in question, and that the content would cause or incite them to become a prostitute by engaging in sex work.

2.252 In our November 2023 Consultation we recognised that most services providers are unlikely to be able to know whether or not their users are already sex workers. However, we consulted on our view that this is not always a barrier to them drawing a reasonable inference that content incites prostitution, as most users of most U2U and search services are not working as sex workers. However, we thought that an exception may arise in relation to services (or accounts within services) which are specifically dedicated to sex work, where it is conceivable or even likely that the majority of users viewing the advertisements in question are already engaged in sex work.

2.253 **Nordic Model Now!** argued in its response that our assumption that only sex workers would access services dedicated to sex work was "incorrect and misguided."106 It argued that people, particularly children and young people, will be attracted to these types of services as they are likely to be curious about sexual matters.107

2.254 In our final ICJG, we have adopted the view that it is reasonable to infer that most users of user to user and search services are not already sex workers. However, we accept that users of sites dedicated to sex work may include children, and note in addition that buyers of sex are likely to access such sites. We have therefore not included this exception in our final ICJG.

Controlling a prostitute for gain

Use of Sexual Trafficking Identification Matrix (STIM)

2.255 In our November 2023 Consultation on the offence of controlling a prostitute for gain, we set out that we had considered whether there are any 'warning signs' that may indicate that a sex worker is being controlled for gain by another person or persons. We provisionally concluded that the indicators we considered were not determinative signs of control, because such indicators may also be present in arrangements which are unlikely to amount to control, including where sex workers had taken steps to promote their own safety. We were conscious that if we were too prescriptive in our guidance on this offence, we risked undermining sex workers' efforts to keep themselves safe online, possibly driving them to less safe environments.

2.256 Some consultation respondents expressed concern about the prevalence of exploitation and our position on this point.[108] Since publishing our November 2023 Consultation, we

---

[105] *R v Ubolcharoen* [2009] EWCA Crim 3263.
[106] Nordic Model Now! response to November 2023 Illegal Harms Consultation, p. 18.
[107] Nordic Model Now! response to November 2023 Consultation, p. 18.
[108] [✂]. Vivastreet response to November 2023 Consultation, p. 4.

have also been presented with evidence suggesting that where certain indicators are present, this may be a clear sign that an individual is being exploited.[109]

2.257 [✂].[110] One of the main concerns raised was that sex workers would not be able to advertise services online anymore, for instance because their ads would be removed or because adult service websites ('**ASWs**') would shut down completely, and that this would mean that sex workers would be pushed to offline spaces where they are more at risk of harm.[111]

2.258 Further, in a report shared with Ofcom by the Sex Workers Union in its response to the November 2023 Consultation, Hacking//Hustling looked at the consequences of the FOSTA-SESTA bill which became law in the United States in 2018. The stated aim of this law was to reduce human trafficking, however the report argues that this law put pressure on Internet platforms to "censor" their users. As a result of this, the sex worker communities that this law directly impacted claimed it pushed them off reliable and trusted platforms, and thereby increased their exposure to violence, leaving those who rely on sex work as their primary form of income without many of the tools they had used to keep themselves safe.[112] The Sex Worker Union also shared other evidence which argues that FOSTA-SESTA has made legitimate sex work less safe.[113]

2.259 In its response, Changing Lives recommended that the ICJG refers service providers to the Sexual Trafficking Identification Matrix (STIM) as a mechanism for identifying indicators of sexual exploitation within advertisements.[114] This tool was created to help police forces identify adverts posted on ASWs that show a high, medium or low risk of exploitation, and is now also used by a handful of non-governmental organisations.[115] The tool is based on a scoring system and if a piece of content has a score of 30 points or more, the STIM classifies this as being at high risk of being exploitative. In meetings with Dr Xavier L'Hoiry (Sheffield University), Dr Alessandro Moretti (University of Copenhagen) and Professor Georgios A. Antonopoulos (Northumbria University) who created and developed the STIM, they highlighted to Ofcom that there is always a risk of false positives being flagged when using the STIM, meaning it could identify content posted by independent sex workers who are not being exploited and controlled. However, they said they were confident about the small chance of false positives in content that shows a high risk of exploitation. They noted that their priority in the last year or so has been working on reducing the chance of false positives from using the STIM.[116] They informed us that, although it was not developed for a regulatory purpose, the tool is flexible and allows experienced and non-experienced users to determine whether an advert on an ASW is low, medium or high risk.[117]

---

[109] All Party Parliamentary Group on Commercial Sexual Exploitation, 2024. Men Who Buy Sex. [accessed 18 September 2024]. Home Affairs Select Committee, 2023. Human trafficking. [accessed 18 September 2024]. Sanders, T. 2023. The role of adult service websites in addressing modern slavery. [accessed 23 October 2024].
[110] [✂].
[111] [✂].
[112] Blunt, D. & Wolfe, A. 2020. Erased: The Impact of FOSTA-SESTA. [accessed 26 November 2024]. See also our Register of Risk chapter 'Sexual Exploitation of Adults'.
[113] Albert, K., et al. 2021. FOSTA in Legal Context. [accessed 26 November 2024]. Chamberlain, L. 2019. FOSTA: A Hostile Law with a Human Cost. [accessed 26 November 2024].
[114] Changing Lives response to November 2023 Consultation, p. 16.
[115] Ofcom/Xavier L'Hoiry, Alessandro Moretti, Georgios Antonopoulos meeting, 7 June, 2024.
[116] Ofcom/Xavier L'Hoiry, Alessandro Moretti, Georgios Antonopoulos meeting, 5 September, 2024.
[117] Ofcom/Xavier L'Hoiry, Alessandro Moretti, Georgios Antonopoulos meeting, 7 June, 2024.

2.260 Based on this new evidence, we have reviewed our approach to indicators of exploitation. The evidence focuses on ASWs but we are aware of no reason for indicators to be different on other services, and sexual exploitation does not just happen on ASWs. We have therefore taken the view that indicators may be applicable to all in-scope services.

2.261 We consider that where there are a large number of indicators of exploitation, relied on both by law enforcement and non-governmental organisations, it is reasonable to infer that content is illegal. In our final guidance, we therefore steer service providers to consider a modified version of the STIM indicators when making illegal content judgements. We say that posts that are classified as high risk under the STIM are highly likely to be illegal and service providers should, absent evidence to the contrary, have reasonable grounds to infer that content is illegal.

2.262 We recognise there is a risk that content on services showing a high risk of exploitation has actually been posted by an independent sex worker, and that, as set out in paragraph 2.258, the wrongful removal of their content may harm an independent sex worker both financially and in terms of safety. However, we now believe that there are likely to be materially fewer false positives than true positives. In addition, as set out in chapter 6 of our Codes of Practice (Volume 2), service providers should have an easy to find, easy to access and easy to use complaints system. This should provide independent sex workers with an avenue to appeal in the event that their content is wrongfully removed, thereby reducing the risk that the application of the STIM inadvertently gives rise to harm. We note that the potential benefits to sex workers of advertising via a third party do not obviate the need for systemic assessment of the risks that may be indicated by advertising sex work in this way, however steer service providers to consider the risk that independent sex workers often post content online which may include the indicators outlined in the STIM. They may do so for a variety of reasons, including safety reasons, and we have therefore asked service providers to take into account any information provided as a result of user reports or appeals, like for instance appeals from independent sex workers.

Image-based adult sexual offences

2.263 The priority image based adult sexual offences are possession of extreme pornography (Section 63 of the Criminal Justice and Immigration Act 2008) and intimate image abuse (Section 66(B) of the Sexual Offences Act 2003). We also consulted on guidance relating to the non priority offence of cyberflashing (Section 66A of the Sexual Offences Act 2003).

Acts which threaten a person's life and extreme pornography offence

2.264 One kind of extreme pornography is pornography which portrays, in an explicit and realistic way, an act which threatens a person's life. In the draft guidance on the extreme pornography offence we said that content which depicts hanging, suffocation or sexual assault involving a threat with a weapon are likely to portray an act which threatens life. We also said that acts of choking or strangulation do so only where the act is extreme, persistent and appears to represent a credible threat to life and that consensual acts of bondage, domination and sadomasochism are unlikely to threaten life except where they involve any of the aspects previously mentioned.

2.265 An individual respondent and the **Victims' Commissioner for England and Wales** both expressed concern about this approach, more specifically what we said about depictions of

strangulation.[118] They argued that we had set the bar too high, citing medical evidence and coroners reports that strangulation can cause serious injury and threaten life at a much lower threshold. As a result of the concern expressed in the stakeholder responses, we have reassessed our drafting around acts which threaten a person's life. Aligned with legislation and stakeholder concerns around the draft ICJG as it related to strangulation, our final guidance sets out that acts which threaten a person's life mean acts which depict physical endangerment with a material risk of death. Non exhaustive examples include explicit and realistic hanging, strangulation, suffocation and causing life threatening injury, meaning that content which depicts this would be likely to be illegal.

Jurisdiction and intimate image abuse offence

2.266 The intimate image abuse offences in England/Wales and Scotland are similar to one another, but not identical. For the purpose of identifying illegal content, it does not matter what country a user is posting the content from if the service it is being posted to is being regulated by Ofcom. In effect, content is illegal content if it amounts to either the English/Welsh offence or the Scottish offence.

2.267 However, considering each offence separately in turn is likely to be onerous for providers and may be confusing to content moderation teams as well. After careful thought about the similarities and differences between the offences, we have decided to collapse the two offences together, led mostly by the English/Welsh version of the offence which on balance we consider likely to be identifiable first.

2.268 The key differences between the offences are:

a) **Consent:** the principal reason why the English/Welsh offence is easier to consider than the Scottish one is that to show the Scottish offence, the service would need 'reasonable grounds' on which to infer a negative - that the photograph or film concerned has not previously been disclosed to the public at large, or any section of the public, by the individual or with the individual's consent. While it would be possible to build a content reporting form which asked this question specifically, we are not aware that service providers generally do, so they may have no information on previous disclosure. By contrast, the English/Welsh offence only requires positive evidence about consent in relation to the content itself. In many cases reasonable grounds to believe that the disclosure was non-consensual are likely to be provided by the fact of there being a complaint from the person depicted, or by contextual information around the content. We therefore conclude that the English/Welsh offence is likely to be easier to show.

b) **What content is caught:** the English/Welsh definition of the offence is both more detailed and broader than the Scottish one. It captures a photograph or film if it shows or appears to show the person participating or engaging in an act which a reasonable person would consider to be a sexual act; the person doing a thing which a reasonable person would consider to be sexual; all or part of the person's exposed genitals, buttocks or breasts; the person in an act of urination or defecation, or the person carrying out an act of personal care associated with the person's urination, defecation or genital or anal discharge. The reference to all or part of a person's 'exposed' genitals, buttocks or breasts includes a reference to all or part of them being visible through wet or otherwise transparent clothing, them being exposed 'but for the fact that they are

[118] McGlynn, C. response to November 2023 Consultation, p. 3. Victims' Commissioner for England and Wales response to November 2023 Consultation, p. 9.

covered only with underwear', and them being exposed 'but for the fact that they are obscured, provided that the area obscured is similar to or smaller than an area that would typically be covered by underwear'. This is broader than the Scottish offence in that it definitely captures deepfakes, in that it captures urination/defecation and associated personal care which may not be sexual, and in that it captures exposure through wet clothing or obscuring.

c) **State of mind:** the English/Welsh offence occurs when the user uploading the content does not 'reasonably believe' that the person depicted consents. The Scottish offence applies the Scottish definition of recklessness. A person is reckless as to whether the disclosure would cause fear, alarm, or distress if they 'failed to think about or were indifferent as to' whether the disclosure would have that result. However, we have concluded that for the purposes of the ICJG in practice, on the information likely to be available to service providers, this is likely to be a distinction without a difference. A person who failed to think about or was indifferent as to causing fear, alarm or distress would not have reasonable grounds to believe in consent, and the basis for providers to draw either inference is likely to be the same.

State of mind and the intimate image abuse offences

2.269 Intimate image abuse relates to the non-consensual disclosure of, or threats to disclose, intimate images.

2.270 In the November 2023 Consultation, we noted that the definition of illegal content means that when a piece of content is shared, forwarded or reposted by a new user, this is a new piece of content for the purpose of an illegal content judgement. The **OSAN** disputed this, arguing that it is an overly restrictive reading of the Act, and that section 59 only requires there to have been a link "at some stage."[119]

2.271 We remain of the view that the definition of illegal content means that when a piece of content is shared, forwarded or reposted by a new user, this is a new piece of content for the purpose of an illegal content judgement. The definition of an illegal content judgement requires inferences to be drawn about state of mind. In addition, many priority offences require offline circumstances to be present for an offence to be committed, and whether or not those circumstances are present may be different when content is shared, forwarded or reposted. Some priority offences are committed or not depending on the nature of the person who posts the content or who sees the content. It follows that when reposted or reshared, it must be possible for content to cease to be illegal content. And finally, it is difficult to see how defences could be considered, since they are specific to the user relying on them. We also note that the consequences of a reading which meant that content once illegal stayed illegal would be significant. It would impact on, for example, journalism, political speech, satire and creativity. And it would suggest that content once not illegal, could not become illegal when reposted by someone in the right circumstances and with the right intent.

2.272 In our November 2023 Consultation on intimate image abuse, we proposed that when a piece of content identified as intimate image abuse was shared, forwarded or reposted, it may not always be possible to infer that the state of mind requirements were met. We consulted on wording suggesting occasions when it would be possible to draw this

[119] OSAN response to November 2023 Consultation, Annex D, page 7.

inference, and said that for data protection reasons, where content was known to have been posted without consent, it should be taken down.

2.273 The **OSAN, Refuge** and an individual expressed concern about this approach, arguing that providers should be required by the Act to remove all intimate images known to be non-consensual. [120]

2.274 We revisited the offence in light of these submissions. We note that the state of mind requirement for the English version of the offence is that the user concerned does not "reasonably believe" in consent and that whether a belief is reasonable is to be determined having regard to all the circumstances including any steps the user has taken to ascertain whether there is consent. Considering this, we think it is reasonable to infer that absent any evidence that the user reposting, forwarding or resharing content has taken appropriate steps to ascertain consent, they do not have a reasonable belief in consent. It follows that if the content concerned is an intimate image which has been shared without consent, it will be illegal content when it is forwarded, shared or reposted. Our final Guidance reflects this position.

Cyberflashing offence and inferring state of mind

2.275 Cyberflashing refers to the unsolicited sending of a photograph or film of someone's genitals to someone through digital communication channels. Whilst a person of any gender may be victim of cyberflashing, evidence shows that this behaviour disproportionately affects women and girls, and that a majority of the perpetrators are men.[121] Cyberflashing can cause victims severe distress, and often leaves victims feeling unsafe, vulnerable and upset. We are committed to reducing harm from cyberflashing as part of our wider effort to make the online space safer for women and girls.

2.276 In the draft Guidance, we stated that the state of mind element of this offence (intent to cause distress, alarm, or humiliation or, where the photograph or film is sent for the purpose of obtaining sexual gratification, recklessness as to whether alarm, distress or humiliation would be caused) is unlikely to be reasonably inferred in most cases, except where there is explicit evidence of the intent behind sending the message.

2.277 **The OSAN, Refuge**, and an individual all expressed concern with our proposed approach in their response, arguing that the threshold is too high.[122] An individual and the **OSAN** argued that Ofcom should place weight on the harm caused by such images.[123] They said that although limited, evidence suggests that a proportion of men who send genital imagery send it knowing it could be seen as distressing or threatening. In particular, the individual stakeholder cited research suggesting that 29% of millennial men surveyed who have admitted to sending genital imagery thought women would describe it as "distressing" and 24% thought that women would describe it as "threatening".[124] The same stakeholder also noted a more recent study suggesting that of the Canadian men surveyed admitting to

---

[120] McGlynn, C. response to November 2023 Consultation, p. 16-17. OSAN response to November 2023 Consultation, Annex D, p. 7. Refuge response to November 2023 Consultation, p. 25.
[121] See the chapter of the Register of Risk titled 'Non-priority offence: Cyberflashing.'
[122] OSAN response to November 2023 Consultation, p. 8. Refuge response to November 2023 Consultation, p. 25. McGlynn, C. response to November 2023 Consultation, p. 14-15.
[123] OSAN response to November 2023 Consultation, p. 8. McGlynn, C. response to November 2023 Consultation, p. 14-15.
[124] YouGov (Smith, M.), 2018. Four in ten female millennials have been sent an unsolicited penis photo. [accessed 3 September 2024].

sending such imagery, 15% were aiming to induce fear.[125] The stakeholder submitted that these studies are limited, relying as they do on self-reporting (because people do not like to identify themselves as bad).

2.278 We recognise the concerns raised by stakeholders in their responses. We do not consider that the evidence provided, on its own, gives us a basis on which to say that there are reasonable grounds to infer a criminal state of mind in the case of all sending of genital imagery, nor do we accept that we are entitled to do so merely because such content is harmful. But we do accept that the studies are likely to under-report – perhaps significantly – the prevalence of a criminal state of mind. We also consider that a more careful assessment of the context in which such images are sent, and are likely to come to the attention of service providers, is helpful.

2.279 Genital imagery can in some instances be received consensually. The evidence cited shows that in some instances women solicit the content and that a proportion of both men and women consider such images can be 'sexy'.[126] However, in these cases there is likely to be a prior relationship between the sender and the receiver, and it is more likely that the people concerned will be using private channels of communication which are unlikely to come to the attention of a service provider absent a complaint. In other words, these more benign scenarios are less likely to be a part of the universe of content which a content moderator will need to consider. Similarly, communities within which it is an accepted part of the culture for people to send unsolicited genital imagery are also unlikely to generate much content for moderation.

2.280 We consider that the likelihood of intent or recklessness is significantly greater on services and within communities where sending unsolicited genital imagery is not an accepted part of the culture. In our final guidance, we have therefore said that it is likely to be reasonable for service providers to infer the required intent or recklessness where a user sends content depicting genitalia, unless:

a) There is good evidence of consent from the user(s) receiving the photograph or film; or
b) It is posted on a service where it is a commonly accepted part of the culture to send and receive intimate images without prior agreement.

Expanding guidance on cyberflashing to section 127(1) of the Communications Act 2003

2.281 One individual recommended in their response to the November 2023 Consultation that the guidance on cyberflashing should be expanded to include section 127(1) of the Communications Act 2003 ('Improper use of public electronic communications network') arguing that cyberflashing content which does not meet the threshold for illegality through the cyberflashing offence, is highly likely to be considered illegal content under the section 127(1) offence.[127]

2.282 We do not think it would be appropriate to ask providers to treat all images of genitalia as the section 127(1) offence since this would suggest the content would be illegal even if

[125] Oswald, F., Lopes, A., Skoda, K., Hesse, C. L, Pedersen, C. L. 2020. I'll Show You Mine so You'll Show Me Yours: Motivations and Personality Variables in Photographic Exhibitionism. *The Journal of Sex Research* 57 (5), [accessed 3 October 2024].
[126] YouGov (Smith, M.), 2018. Four in ten female millennials have been sent an unsolicited penis photo. [accessed 3 October 2024].
[127] McGlynn, C. response to November 2023 Consultation, p. 13-14.

actively solicited or welcomed by the recipient, and would tend to suggest that all pornography was illegal. This would have serious freedom of expression repercussions.

Unlawful immigration and human trafficking

2.283 The Act contains five priority offences to do with immigration and human trafficking. They are offences relating to illegal entry into the UK; facilitating unlawful immigration; and the human trafficking offences. These priority offences centre around an individual being involved in the illegal movement of people, either across borders or within countries.

Separation of human trafficking and unlawful immigration chapters

2.284 In the draft ICJG, we covered offences relating to assisting and encouraging unlawful immigration and offences relating to human trafficking within one chapter. We decided to do this because we believed the offences were thematically linked due to the connection between irregular migration and human trafficking.

2.285 The **Global Alliance Against Traffic in Women (GAATW)** argued that the sections on unlawful immigration and human trafficking should be separated as these are "two totally distinct legal and factual concepts."[128] Another stakeholder [✂] called for greater demarcation between unlawful immigration and human trafficking in the consultation more generally.[129] We acknowledge and agree with these points. In our updated Guidance, we have split the chapters on human trafficking and unlawful immigration to ensure that the offences are kept conceptually distinct.

Human trafficking

Definition of human trafficking

2.286 The draft ICJG included a broad definition of human trafficking derived from the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons (the 'Palermo Protocol'), alongside a more specific legal outline of the offence of human trafficking as it exists under UK law. This included further detail on the types of 'exploitation' as defined by UK statute.

2.287 The **Global Alliance Against Traffic in Women (GAATW)** queried this definition of human trafficking, arguing that it is inconsistent with the international legal definition and the definition under the Modern Slavery Act 2015, as it singles out certain forms of exploitation and not others.[130]

2.288 As explained in the November 2023 Consultation, our guidance must comprise the statutory definitions of exploitation under not just the Modern Slavery Act 2015, but also (as required by the Act) the Human Trafficking and Exploitation (Scotland) Act 2015 and Human Trafficking and Exploitation (Criminal Justice and Support for Victims) Act (Northern Ireland) 2015. Our view is that the Scottish version of the human trafficking offence is broader than the English/Welsh and Northern Irish ones, and we have therefore focused mostly on that offence in our guidance. We have decided there is no need to define the offences, since describing them is sufficient. When making content judgements in relation

[128] Global Alliance Against Traffic in Women (GAATW) response to November 2023 Illegal Harms Consultation, p. 27.
[129] [✂].
[130] Global Alliance Against Traffic in Women (GAATW) response to November 2023 Consultation, p. 28.

to potential human trafficking content, service providers should refer to paragraphs 11.4-11.5.[131]

2.289 The Scottish version of the offence takes place when a person (Person A) takes a 'relevant action' with a view to another person (Person B) being exploited. 'Relevant actions' online are most likely to be the recruitment of another person, or the arrangement or facilitation of acts of transport or transfer, or of harbouring, or of receiving of another person – so long as all of these actions are done with a view to exploiting the person involved. 'Exploiting' is a defined term which we set out in detail in our guidance on the offence.

Jurisdiction

2.290 The offence contains a number of different provisions relating to jurisdiction/connection to the UK. However, amongst them is the provision that the offence is committed if 'any part of the relevant action takes place in the UK'. We consider that this will always be met in the case of online content and therefore do not discuss it in our guidance. This is because content is only illegal content if it 'amounts' to the offence, so there can be no conceptual distinction between the content and the 'relevant action'. If the content is accessible to users in the UK, the relevant action will take place in the UK. And, in any event, the Act provides that for the purposes of determining whether content is illegal content, it does not matter whether anything done in relation to it takes place in any part of the UK. The Explanatory Note to the Act confirms that this means content will 'amount to an offence' regardless of whether the criminal law would require the offence, or any element of it, to take place in the United Kingdom (or a particular part of it).

2.291 We have therefore concluded that reasonable grounds to infer that content amounts to an offence are likely to exist where content makes explicit reference to the exploitation of another person.

Thresholds for illegality in the case of human trafficking

2.292 As part of our guidance on human trafficking and the 'controlling prostitution for gain' offences, we said perpetrators of such offences are unlikely to be honest about their intentions to exploit others, and – as such – service providers should have regard to evidence provided by UK law enforcement agencies where it is available. We took this approach in order to steer providers towards a viable basis for establishing 'reasonable grounds to infer', even where evidence of intent to exploit is not clear or available.

2.293 **Vivastreet**'s response expressed concern that our proposals "set the bar too low" for 'adult services websites' (ASWs) by stating that service providers are unlikely to reach reasonable grounds to infer content amounts to the human trafficking offence and sexual exploitation of adult offences unless notified by law enforcement.[132]

2.294 As Vivastreet's concerns primarily relate to trafficking for sexual exploitation on ASWs, we believe the 'controlling prostitution for gain' offence is more relevant in addressing its concern (the guidance on this offence is covered in chapter 9 on 'Sexual exploitation of adults'). As set out in paragraphs 2.256-2.263, we have made several changes to the guidance on this offence. In summary, we have decided to ask providers to ordinarily judge content which shows a high risk of sexual exploitation using the Sexual Trafficking Identification Matrix (STIM) indicators (for more information about the STIM tool, see

[131] Human trafficking is not a legal term, it is just a way to refer to the offence.
[132] Vivastreet response to November 2023 Consultation, p. 3.

paragraph 2.260) as amounting to the 'controlling prostitution for gain' offence. Please see more detail about our reasoning for doing so in paragraphs 2.256-2.263.

2.295 We are acutely aware that independent sex workers who use in-scope services to operate safely and legally may be threatened both financially and in terms of their safety as a result of 'over moderation' or blanket approaches which suggest that indicators which are *associated* with exploitation may be used to *reasonably infer* exploitation (and thus to remove content). In our guidance on the 'controlling prostitution for gain' offence we therefore ask providers to be aware that independent sex workers often post content online which may include the indicators outlined in the STIM, and ask them to take into account any information about intent provided as a result of user reports or appeals, like for instance appeals from independent sex workers.

Unlawful immigration

2.296 The offences relating to illegal entry into the UK cannot themselves be committed online as it is not possible for a person to 'enter the UK' except physically. However, the related offences of 'encouraging', 'assisting' or (if two or more people are involved) 'conspiracy' or 'being involved art and part' may be relevant. The state of mind requirements for these offences is high (including 'intent'), and the analysis is complicated by the fact that, for example, it is not necessarily unlawful to cross the Channel or to invite others to take trips by boat.

Non-UK immigration law

2.297 In our November 2023 Consultation, we noted that the offence of facilitating unlawful immigration is only committed where the content posted amounts to an 'act' that facilitates the breach or attempted breach of immigration laws in a range of different countries, and the person posting it has knowledge or reasonable cause for believing that the individual whose breach is facilitated is not a national of the United Kingdom. We said that the range of possible acts which might facilitate the commission of such a breach is very broad, but it is difficult to see how any of them could be committed online. We noted that applying the offence in practice would require service providers to have a detailed knowledge of the immigration laws in many countries and that it would not be proportionate for us to do so.

2.298 One stakeholder [✂] argued in its response that providers do not need to have a detailed knowledge of immigration laws of many countries to know that the organised immigration crime services being advertised are offences in most if not all countries.[133] It argued that the relevant jurisdiction and law cannot necessarily be determined by the service providers given that organised immigration crime by its very nature impacts multiple countries.[134]

2.299 While we recognise that crossing borders without required authorisations is generally illegal, we are not in a position to give guidance on legislation in other countries and we consider that in order to make illegal content judgments a provider would, at least, need to know when authorisations are required. At this stage, we are therefore not making any changes to the ICJG in relation to this. As set out below in paragraphs 2.302-2.303, and in the ICJG chapter on the unlawful immigration offences, when false documents are used to

[133] [✂].
[134] [✂].

commission an unlawful immigration offence, service providers should consider whether this amounts to the 'articles for use in frauds' offence.

Safety advice and support for irregular migrants

2.300 As part of its response, the **Global Alliance Against Traffic in Women (GAATW)** highlighted the lack of guidance on how service providers should handle "online information designed to assist irregular migrants that is shared for the purpose of protecting their health and wellbeing, or ensuring that they are able to access identification procedures for victims of trafficking and refugees."[135] We acknowledge this gap and have decided to include guidance on how to treat such content in our updated document to make it clear that such content does not amount to an offence and should not be treated as illegal content.

Role of false documentation

2.301 One stakeholder [✂] argued that the ICJG does not sufficiently convey the relevance of false documentation in organised immigration crime.[136] The drafting provided on this topic in the draft ICJG was limited for practical purposes, in order to keep unnecessary explication to a minimum and concentrate on how service providers should approach certain types of content. In this case, the ICJG instructs providers to consider any content advertising the sale of false documents in relation to fraud offences (specifically, articles for use in frauds), rather than unlawful immigration offences (specifically, assisting illegal entry). This is because the reasonable inferences which need to be made in relation to the relevant fraud offence are simpler to establish and require more readily available information than those that need to be made in relation to the unlawful immigration offence.

2.302 In response to the stakeholder's concern, we have added some additional explanation as to the role of documentation in immigration crime, to support this signposting.

Encouraging or assisting suicide and serious self-harm

2.303 We have made extensive changes to our chapter on assisting or encouraging suicide and serious self-harm. Broadly, these changes are intended to: be more nuanced in our approach; emphasise the importance of considering safeguarding and support in the moderation of suicide and self-harm content; and ensure that the language used is appropriately sensitive.

2.304 As a result of our decision regarding non-priority offences, we have separated the chapter on assisting or encouraging suicide and serious-self harm into two: one covering the suicide offence, and one covering the serious self-harm offence.

2.305 Although they are distinct offences, and now separate chapters, the changes made to our guidance on one group of offences is often appropriately carried over to the other. We have set out changes to the suicide offences most extensively in the section titled 'Assisting and encouraging suicide', and readers should note that these are often mirrored in the self-harm chapter. To avoid unnecessary repetition, we have provided the full details only once.

Assisting and encouraging suicide

Scope of content covered by guidance on suicide offence and nuance in drafting

2.306 Content amounting to a priority offence of assisting or encouraging suicide is illegal only when there are reasonable grounds to infer intent to assist or encourage.

---

[135] Global Alliance Against Traffic in Women (GAATW) response, 2023, pp. 27-28.
[136] [✂].

2.307 In preparing guidance on the offences related to suicide and serious self-harm, we were mindful that freedom of expression protects many types of lawful content related to the discussion of suicide. In the draft ICJG, we therefore described types of content which we do not consider to be illegal content, as well as types of content which may be. We also discussed in some detail the basis on which a reasonable finding may be made on the state of mind of intent. We considered the context to be particularly important here. We proposed that, where specific, practical or instructive information on how to end one's life is posted to a forum or within a chat in which suicidal ideation is discussed, it may be reasonable to infer that intent to assist (attempted) suicide exists by virtue of information having been posted. Where an encouragement to end one's life is posted in response to what appears to be a credible threat by another user that is about to take their own life, it may also be reasonable to infer intent.

2.308 In its response, **Samaritans** challenged the breadth of content which could theoretically be judged to be illegal content as a result of the draft ICJG on the encouraging and assisting suicide offences.[137] **Samaritans** argued that the draft Guidance lacked nuance, and that it did not demonstrate an understanding of the perspectives of people engaging with suicide content.[138] We recognise this broad point, and have revisited our chapter on the suicide offences to be more nuanced where appropriate. The changes we have made are set out in more detail in the section entitled 'Vulnerability of users posting and engaging with suicide-related content, particularly children.'

2.309 **Samaritans** argued that Ofcom's guidance should refer to the discussion of the meaning of the suicide (and serious self-harm) offences during the Parliamentary passage of the Act, "in order to set out judgements which better reflect the nuances and vulnerabilities involved."[139] While we recognise there was extensive debate about these offences, Ofcom's guidance must reflect the law.

2.310 In particular, **Samaritans** were concerned that a lack of clarity in the draft Guidance around how '"the nature of the post and context around the post" could indicate intent would lead to service providers choosing to remove *all* suicide content, which would risk a negative impact on those seeking supportive spaces online.[140] **Samaritans** also pointed out that, although the section on serious self-harm contained guidance on how providers should treat content describing personal experiences, this was not duplicated in the suicide section. It argued that it is inappropriate to infer intent to assist or encourage where discussion of suicide methods is being framed in the context of personal experience, as it is "entirely possible that people talking about their own lived experience mention methods and this is not automatically illegal content."[141]

2.311 We recognise the risk raised by **Samaritans**. In our final ICJG, we have therefore added text which makes it clearer how providers should make judgements about intent. In particular, we have drawn out more clearly that content which may, on its face, encourage suicide may not be illegal content, because there may be no intent. We state that it is unlikely to be appropriate to infer intent to encourage a person to take or attempt to take their own life where a user responds to a post in which another user expresses an intention to take their

[137] Samaritans response to November 2023 Illegal Harms Consultation, pp. 5-6.
[138] Samaritans response to November 2023 Illegal Harms Consultation, p. 1.
[139] Samaritans response to November 2023 Consultation, p. 7.
[140] Samaritans response to November 2023 Consultation, p. 6.
[141] Samaritans response to November 2023 Consultation, pp. 6-7.

own life with discussions of their own personal experiences with suicide, including suicide attempts. By contrast, we state that acts of 'egging on' may be illegal, especially where such behaviour is targeted or persistent, and have decided to add that this could include "praising someone's stated intention to take their life, as well as more concerted efforts to encourage someone to take a course of action they are not yet committed to." As detailed in the ICJG, this could involve "a scenario in which a user posts that they are considering taking, or intend to take their own life and another user responds with words to the effect of 'you should do it' or that they hope that the person 'succeeds' in taking their own life)."

2.312 In our review of the draft ICJG we have also decided to make changes to our guidance on assistance. We have decided to add drafting to state that content which include details on the most effective way of taking one's own life, or tips about how to do so in a way which avoids interruption from others or to beat a 'survival instinct', is likely to be capable of constituting assistance for the purposes of this offence in an online context.

2.313 We have also decided to clarify that it is unlikely to be appropriate to infer intent where suicide methods are being discussed in the context of personal experience, as opposed to being recommended to another person, *unless* the user encourages other users to try the suicide method they are discussing.

Vulnerability of users posting and engaging with suicide-related content, particularly children

2.314 The draft ICJG included some limited comments regarding the vulnerability of users posting and engaging with potentially illegal suicide content, but these were not drawn out particularly clearly in the text. **Samaritans** were critical of the approach taken in the chapter on suicide-related content, arguing that it lacked nuance and didn't demonstrate understanding of the perspectives of those engaging with such content.[142]

2.315 We have decided to add a new section to the chapter which emphasises the complexities and nuance of moderation in this area. In this section we note that suicide-related content is likely to be posted by users in vulnerable and difficult circumstances, and that spaces where the content is posted may be used to connect with other users with similar experiences. We state that, "While this does not negate their duties relating to the takedown of illegal content, providers should be aware that the over-removal of legal or borderline content relating to suicide may have a negative impact on the user posting (for example, by exacerbating feelings of isolation or self-criticism)."

2.316 Responses from **NSPCC (the National Society for the Prevention of Cruelty to Children)**, the **Canadian Centre for Child Protection (C3P)** and an individual respondent drew attention to the particular vulnerability of children both in the consumption of suicide-related content and its generation.[143] **Canadian Centre for Child Protection (C3P)** argued that encouraging and assisting self-harm and suicide behaviours in children "should be considered serious abuse," as children's reasoning and media literacy abilities are still developing and they are therefore "especially susceptible to what they read."[144] However, stakeholders acknowledged that children are also involved in posting this type of content, and are not always able to comprehend the impact in a way that implies intent. Both the **Canadian Centre for Child Protection (C3P)** and an individual respondent argued that

[142] Samaritans response to November 2023 Consultation, p. 1.
[143] NSPCC response to November 2023 Consultation, p. 51. Canadian Centre for Child Protection (C3P) response to November 2023 Consultation, p. 33. Graham, Dr R. response to November 2023 Illegal Harms Consultation, p. 2.
[144] Canadian Centre for Child Protection response to November 2023 Consultation, p. 33.

children may be less likely to understand the harm they may be inflicting by posting self-harm and suicide content, with the **Canadian Centre for Child Protection (C3P)** calling for "special considerations for children in this area" and the individual respondent noting the need for cognitive development, development stage and health knowledge when assessing intent in relation to self-harm and suicide content.[145]

2.317 Ofcom is acutely aware of the vulnerability of children to self-harm and suicide content, and of the heightened risk they have of being harmed by such content, and in causing harm to others. We have added a new section to our final guidance which sets out the particular vulnerabilities of users posting and engaging with this content, and have highlighted children in particular as a vulnerable group: "Particularly in the case of children or young people, users may not have a full understanding of the harm which may arise from content they are posting."

2.318 We are sympathetic to the argument that, in many cases, child users in particular may not understand the risks inherent in what they are posting, and that this may be used to reason that they do not *intend* to assist or encourage. We have decided to add a line in our final guidance which states: "Where content has been judged to be illegal, we also encourage providers to consider the provision of support services at point of takedown."

Language

2.319 We endeavoured to ensure that the language used in our ICJG chapter on suicide-related content was as sensitive as possible. However, we recognise that there was room for improvement, and have reviewed our entire chapter to ensure that the language matches best practice.

Assisting suicide: URLs

2.320 We have added additional wording on URLs when it concerns assisting the offence with intent. In the final statement we state that content which consists of a URL without any accompanying text may amount to assistance, if the context is such that intent can be reasonably inferred.

Assisting and encouraging serious self-harm

2.321 Many of the points raised and addressed in relation to the ICJG's chapter on illegal suicide content also apply to the equivalent chapter on the non-priority offence of assisting or encouraging self-harm. The points discussed in this section are specific to the self-harm chapter. It should be noted that, like the equivalent suicide offence, the self-harm offence requires intent to assist or encourage.

Threshold for offence of assisting or encouraging serious self-harm

2.322 In the draft ICJG, we said that "Content which provides specific, practical information on how a person may effectively undertake an act of really serious self-harm may be illegal content if intent can be reasonably inferred." We also said that, in relation to encouragement, "blackmail, or egging someone on" may amount to illegal encouragement of serious self-harm where intent can be inferred.

2.323 In its response, **Samaritans** disagreed with the threshold set by our draft chapter on serious self-harm content, arguing that it was too simplistic and did not consider factors in which

[145] Canadian Centre for Child Protection response to November 2023 Consultation, p. 33. Graham, Dr R. response to November 2023 Consultation, p. 4.

content discussing serious self-harm would not amount to an offence.[146] We have decided to amend our guidance to make it clear that content which seeks to minimise harm amongst those intending to self-harm, or that which is intended to share personal experiences, should not be judged to be illegal. Specifically, we state that intent to encourage or assist should not be inferred where "the intent behind the method information posted can be reasonably inferred to promote harm minimisation or safety promotion (for example, recommending less dangerous ways to self-harm, to counter another suggestion), or where the method is being described in the context of a personal experience (without being promoted for replication by others)."

2.324 **Samaritans** further argued that "malicious intent is key to determining whether the offence of 'encouraging or assisting serious self-harm' has been committed" and that this was not reflected in the proposals in the draft ICJG.[147] Malice is not included in the definition of the offence, so we do not consider that our guidance can reference it. However, our final Guidance states that "Intent to encourage or assist will be most clear where there is evidence of sustained pressure or malicious motivation, and will be most likely to be inferred where content is 'egging on' relevant behaviour, or where it contains blackmail or threats."

Examples of intentional misspellings

2.325 In the draft ICJG, we drew service providers' attention to the prevalence of coded language or 'algospeak' in content discussing serious self-harm. Since publishing the draft ICJG, we have become aware of evidence of a particularly common set of terms used to distinguish between differing severity in cutting behaviour. We have decided to add drafting to our guidance which explains these terms and how they may be used to infer that self-harm is 'serious' (that is, that it amounts to capacity to result in really serious harm and/or severe injury). We recognise the risk that citing these terms may inadvertently alert users to their existence, or to encourage those wishing to evade moderation to stop using these terms and instead adopt others. However, we believe that the balance of risk is such that it is more beneficial to users overall to make service providers aware of these terms so that they can correctly distinguish between self-harm which meets the threshold for 'seriousness' and that which does not.

Foreign interference and false communications

2.326 The foreign interference offence is a new offence created by the National Security Act 2023 which is included in the Online Safety Act as a priority offence. The Online Safety Act also created a new relevant non-priority offence of false communications. As both these offences are new, they lack a body of case law or academic discussion from which Ofcom can draw its interpretation. They are both also likely to be particularly difficult to identify in practice, because they can depend heavily on context and/or information beyond that which is visible on the face of a single piece of content.

2.327 We therefore proposed that the first iteration of the ICJG should describe the offences and, where helpful, set out questions a provider should consider, to help make a judgement about having reasonable grounds to infer that content is illegal.

---

[146] Samaritans response to November 2023 Consultation, p. 6.
[147] Samaritans response to November 2023 Consultation, p. 6.

Foreign interference

Scope and ambition of guidance

2.328 In the draft ICJG, we outlined the three parts of the foreign interference offence and acknowledged that "identifying online content amounting to the foreign interference offence is likely to be challenging, particularly in relation to individual items of content." This is because of the difficulties in attributing or linking individual content or activity to a foreign state. This activity is often covert and can be hard to detect, for example, due to the use of proxies to obscure state actors and their intent.[148] Activity may also be designed to target or amplify discourses related to a range of topics, including domestic ones, by creating a deceptive appearance of authenticity.

2.329 As a result, making links to a foreign power can be difficult. For providers to have reasonable grounds to infer that content is illegal, they must be able to infer all elements necessary for the commission of the offence.[149] For the foreign interference offence, this includes the foreign power condition which entails a link to a foreign power. Even if not carried out by a foreign power, providers would need to have reasonable grounds to infer that content was posted with intent to benefit a foreign power or that a person was engaging in such conduct recklessly.

2.330 We noted that, while proactive technology to detect patterns suggesting foreign influence may help to identify illegal foreign interference content, such technology may not be available to many service providers. We added that "Absent this type of technology, we expect that evidence would need to be provided by UK law enforcement agencies or other credible third parties, for services to draw reasonable inferences."

2.331 We also did not propose to make specific recommendations in our Codes of Practice, as we lacked sufficient information to do so.

2.332 In its response, **Logically**, stated it agreed with our conclusion that identifying and judging foreign interference offence content is likely to be challenging, but argued that our statements about the scope to reasonably infer if content amounts to a foreign interference offence do not reflect wider academic or international regulatory opinion (such as frameworks on what 'misrepresentation' may look like).[150] It also drew attention to generic profiles which should be taken into consideration in the ICJG, and pointed out that many platforms have existing operations to identify foreign influence.[151]

2.333 We acknowledge the point raised by **Logically** and recognise that some of the frameworks and existing generic profiles may help providers identify content which could be foreign interference. However, applied at scale, these may also detect content which does not amount to a foreign interference offence. Tactics used by bad actors may not be exclusive to those engaging in foreign interference. These tactics may also only represent some forms of foreign interference. In such cases, information about who is controlling bots, or information about patterns of behaviour of which a single piece of content is part, may help providers to identify content amounting to a foreign interference offence.

2.334 In any event, we are not in a position to give guidance that such information is reasonably available to service providers. Many service providers will not have access to technology

[148] Further analysis of this can be found in our Register of Risk, Chapter 6P: foreign interference offence.
[149] Online Safety Act 2023, Section 192(6).
[150] Logically response to November 2023 Illegal Harms Consultation, p. 21.
[151] Logically response to November 2023 Consultation, p. 24.

such as pattern recognition software. We do not currently have enough information to assess its effectiveness in countering content which might amount to a foreign interference offence.

2.335 For present purposes, our guidance on the foreign interference is based on information that is reasonably available to *all* service providers regardless of their size, capacity or access to further information, because we do not have sufficient evidence of the costs or practicalities of special technologies to be able to make decisions about which providers can reasonably be expected to use them. As such, we believe our draft proposals are proportionate and appropriate given the limitations which providers are likely to be working under and the evidence available now.

Information provided by third parties

2.336 In the draft ICJG, we discussed the types of information that service providers may have access to, and which was relevant, but which may not be reasonably available in all cases. We stated that, in cases where providers do not have access to proactive technology which detects patterns associated with foreign influence, "we expect that evidence would need to be provided by UK law enforcement agencies or other credible third parties, for services to draw reasonable inferences." We have decided to expand upon this statement to provide greater clarity as to how providers should approach information from third parties.

2.337 Our final ICJG now states that: 'We expect that credible evidence from expert third parties can help providers draw reasonable inferences about whether any, or all, of the three conditions in the offence have been satisfied. However, at this stage it is not possible to anticipate what evidence may be available or how it should be interpreted, so as to give detailed guidance on the point.' We furthermore state that, when making content judgements, providers "should ensure that such decisions are made at an appropriate level of seniority and weighing up the importance of freedom of expression against the likely covert nature of any foreign state action."

Clarity and length of foreign interference chapter

2.338 We have made a number of small changes in relation to the chapter on Foreign Interference in order to make the drafting more streamlined and to clarify and correct legal points where appropriate. This includes adding definitions of 'course of conduct' and an explanation of the importance of the 'foreign power' condition.

References to fraud and stirring up hatred offences

2.339 When reviewing our guidance, we noted that there is a possible overlap between potential foreign interference offence content and content which could amount to offences of stirring up hatred and/or fraud by false representation.

2.340 In the introductory section of the Foreign Interference chapter, we have therefore decided to add references to the relevant sections to draw providers' attention to the possible need to consider these offences in addition.

False communications

Impacts on freedom of expression

2.341 In the draft ICJG, we gave descriptive guidance regarding the non-priority false communications offence, setting out the three parts of each offence and stating that reasonable grounds to infer that content amounts to a false communications offence will

exist where the conduct elements of the offence are satisfied and both of the following are true:

a) the user posting the content knows the content to be false; and
b) the user posting the content intends to cause non-trivial psychological or physical harm.

2.342 We provisionally concluded that it is likely to be challenging for service providers to make judgements based on content alone. Due the complexity of the offence and the particularly high importance of context when making judgements, we also proposed not to give any usage examples of this offence.

2.343 We received a number of responses with regard to the false communications offence, with some stakeholders, for example, **SPRITE+ (University of Sheffield)**, raising concern that the lack of clarity in the ICJG on this offence would risk negative impacts on freedom of expression due to moderators defaulting towards takedown if uncertain.[152] In particular, **SPRITE+ (University of Sheffield)** noted that neither the Act nor Ofcom has defined what "non-trivial psychological or physical harm" in this context. The **British and Irish Law, Education and Technology Association (BILETA)** expressed disagreement with our argument that there is a lack of body of case law or academic discussion on which Ofcom can draw for interpretation of the false communications offence, stating that it has been discussed by the academic community "for a very long time now."[153]

2.344 We acknowledge the concerns raised in regard to freedom of expression and accept that we have made a conscious choice not to give what we consider to be extra detail above and beyond what is clear in legislation. We believe to do so would itself pose a risk to freedom of expression. As stated in our November 2023 Consultation, context is particularly important in the consideration of the false communications offence, and providers are unlikely to be able to make judgements on the basis of content alone. We believe this is the case regardless of academic discussion on the issue.

2.345 For this same reason, we have decided not to act on the recommendation by **X Corp** to provide clear examples of how the offence may manifest in practice.[154] We believe this would be inappropriate due to the highly contextualised nature of these judgements. We are concerned that providing examples would lead to an approach to content which is not sufficiently nuanced.

2.346 In our final guidance, we have made it clear that the provider must consider both:

a) whether there is evidence (either as part of the content or established based on credible information provided by expert third parties) to illustrate that the user posting the content knows the content is false; and
b) whether there is evidence (either as part of the content or established based on credible information provided by expert third parties) that suggests that the user posting the content intends to cause non-trivial psychological or physical harm.

2.347 We also make it clear that a provider is not required to accept the opinions of a third party as to whether content is illegal content. Only a judgement of a UK court is binding on it in

[152] SPRITE+ (University of Sheffield) response to November 2023 Consultation, p. 23.
[153] SPRITE+ (University of Sheffield) response to November 2023 Consultation, p. 23. British and Irish Law, Education and Technology Association (BILETA) response to November 2023 Consultation, p. 22.
[154] X Corp response to November 2023 Consultation, p. 4.

making this determination. In all other cases, it will need to take its own view on the evidence, information and any opinions provided.

2.348 We say in our final ICJG that we anticipate that it will be challenging for service providers to make these judgements based on content alone. We consider that overall, the ICJG makes it clear that it is difficult to infer that the false communications offence has been committed, and our approach to it is consistent with the right to freedom of expression.

False communication and deepfakes

2.349 In its response, the **Good Law Project** stated that 'non-intimate deepfakes, such as those targeted at politicians' could give rise to a false communications offence. The legal advice it commissioned also suggested that Ofcom's draft guidance on the offence was 'deficient'.[155] This is because it did not include examples of contextual information, including in relation to deepfakes, and did not make a judgement on the extent to which the offence captures deepfakes.

2.350 In setting out our approach to this offence, we highlighted that we have not given extra detail beyond that set out in legislation. As the offence is new, we also did not have a body of case law related to the offence which could be drawn on. However, we acknowledge the risks that can be posed by political deepfakes and have added examples of them to our analysis of how harms can manifest from the false communications offence (see the Register of Risks chapter titled 'Non-priority offence – false communications.') We expect providers to consider this analysis when carrying out their risk assessments.

Animal cruelty and torture

2.351 In our August 2024 Further Consultation, we set out our approach to the priority offence of causing unnecessary suffering to a protected animal, section 4 of the Animal Welfare Act 2006 ('**AWA 2006 offence**'). A person commits this offence where they know or ought reasonably to know that their conduct would cause, or would be likely to cause, unnecessary suffering to a protected animal.

2.352 The AWA 2006 which makes it an offence to commit an action that would cause, or would be likely to cause, unnecessary suffering, cannot itself be committed in the form of content. In other words, although online content can clearly depict an act of animal cruelty that would amount to an offence, the content cannot itself cause suffering to an animal. It is not therefore possible for the AWA 2006 offence to be committed online.

2.353 However, in certain limited circumstances, content could amount to an inchoate version of the offence. For example, a user could urge others to commit the offence (encouraging) or give them helpful advice on how to commit the offence (assisting), or plan with others to commit the offence (conspiracy).

2.354 We stated that, on the face of it, there appears to be a risk that, taken in isolation, the priority AWA 2006 offence does not deal with pre-recorded animal cruelty in a suitably robust way. A depiction of animal cruelty may well not amount to priority illegal content, because a depiction alone does not have the characteristics the law requires to say that it is encouraging, assisting or conspiring someone else to commit the offence. It is not possible to encourage, assist or conspire to an action which has already taken place when the act of encouraging, assisting or conspiracy is first done and, as such, "comments applauding pre-

[155] Good Law Project, 'Re: scope for prosecution of Deepfake Dissemination under section 179 of the Online Safety Act 2023' [accessed 18th November 2024].

recorded depictions of animal cruelty will not necessarily amount to priority illegal content." A similar challenge also arises in relation to pre-recorded human torture content.

2.355 However, we said that the same issue does not necessarily arise in relation to livestreaming of acts of animal cruelty. We stated that "a livestream of animal cruelty being carried out, which users choose to watch knowing what they will see, can be characterised as a conspiracy to commit the animal cruelty offence and is likely to amount to priority illegal content."

2.356 Furthermore, we stated that extreme cases of animal cruelty would amount to illegal content under the non-priority offence of improper use of a public electronic communications network (s. 127(1) of the Communications Act 2003), where they depicted serious injury or death of an animal in a way which is 'obscene.'

2.357 Several stakeholders questioned our approach, arguing that it set the bar too high and would result in an unacceptable amounts of animal cruelty content being left online. Respondents making this argument included the **Battersea Dogs and Cats Home**, **Born Free Foundation**, the **Dogs Trust**, **Humane Society International**, **International Cat Care,** the **OSAN**, and the **RSCPA**.[156] The **Born Free Foundation, Humane Society International**, and **Wildlife and Countryside Link** argued our approach was inconsistent with the intention of Parliamentarians when adding the AWA 2006 offence as a priority offence.[157]

2.358 We recognise the limitations of the approach we are taking and acknowledge that it may result in content which depicts the non-obscene suffering of animals being left online. However, Ofcom is required to work within the limits of the law as passed by Parliament. The ICJG is merely setting a minimum standard for the illegal content which the illegal content safety duties apply to. Service providers are entitled to take down content above and beyond what is illegal, so long as they do in compliance with their other duties, and many may choose to do this in relation to animal cruelty content in recognition of the harm caused to users viewing such content. The provisions of the Act on content harmful to children are also relevant. By providing guidance on the s. 127(1) offence, we are also ensuring that services are obliged to take down the most extreme examples of content depicting animal cruelty and human torture, including some which is not covered by the AWA 2006 offence.

The Obscene Publications Act 1959

2.359 Before deciding on our proposal to rely on the s. 127(1) offence, we considered whether it was appropriate to instead rely on section 2 of the Obscene Publications Act (the '**OPA offence**') in order to target real depictions of animal and human murder and torture. Under the OPA offence, it is an offence to publish an obscene article, which is an article which, taken as whole, is such as to tend to deprave and corrupt persons who are likely, having

[156] Battersea Dogs and Cats Home response to August 2024 Further Consultation, p. 9. Born Free Foundation response to August 2024 Further Consultation on Torture and Animal Cruelty, pp. 3-4. Dogs Trust response to the 2024 Further Consultation on Torture and Animal Cruelty, p. 3. Humane Society International response to August 2024 Further Consultation on Torture and Animal Cruelty, p. 4. International Cat Care response to August 2024 Further Consultation, p. 5. OSAN response to August 2024 Further Consultation on Torture and Animal Cruelty, pp. 5-6. RSPCA response to August 2024 Further Consultation, pp. 10-11.

[157] Born Free Foundation response to August 2024 Further Consultation, p. 5. Humane Society International response to August 2024 Further Consultation, p. 4. Wildlife and Countryside Link response to the August 2024 Further Consultation on Torture and Animal Cruelty, pp. 3-5.

regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

2.360 The s. 127 offence and the OPA offence are similar in that they both target obscenity and are both worded broadly by the UK courts. However, there are some differences between the offences which motivated our proposal to focus on the s. 127(1) offence:

a) While both offences are difficult, the s. 127(1) offence is likely to be somewhat easier for providers to understand. The wording of section 2 of the Obscene Publications Act 1959 is older, and we consider that the words 'tending to deprave or corrupt' (when taken without the words added by schedule 6 of the Online Safety Act) are likely to be particularly difficult for service providers to apply in practice.
b) Under Schedule 6 of the Online Safety Act, section 2 of the Obscene Publications Act 1959 is a priority offence – but only if the obscene article in question tends to deprave or corrupt others by encouraging them to commit one of the child sexual exploitation or abuse offences. In our view there is some risk of confusion if we publish regulatory instruments in which the same offence is both a priority and a non-priority offence.
c) Although the s. 127(1) offence is arguably wider than the OPA offence, and therefore may pose more risks to freedom of expression, we think this can be managed by focusing on the parts of it which matter to capture the content which is not caught by other priority offences.

2.361 We also concluded that it would not be appropriate to ask service providers to consider two offences when one would be sufficient.

2.362 We are aware of a successful conviction under the OPA offence in relation to online animal torture content, prosecuted in September 2024.[158] In light of this conviction, we considered whether we should modify our approach but believe that our arguments in relation to the relative strength of an approach relying on the s. 127(1) offence stand. We have therefore decided to go ahead as planned with our proposed approach of relying on s. 127(1) rather than the OPA offence.

Pre-recorded cruelty content as conspiracy or encouragement to commit the AWA 2006 offence

2.363 **Humane Society International**, **International Cat Care,** the **OSAN**, the **RSPCA,** the **Scottish SPCA** and **Wildlife and Countryside Link**, argued against our statement in the August 2024 Further Consultation that only livestreamed acts of unnecessary suffering caused to an animal would amount to conspiracy to commit the AWA 2006 offence.[159] They argued that pre-recorded acts should be within scope an inchoate offence, whether encouragement or conspiracy. The **RSPCA** expressed concern that "the 2024 successful recent Indonesian monkey torture prosecution…may have given an unbalanced view of the propensity and availability of [live acts of animal cruelty] on social media outlets."[160] **SMACC** argued that, in many cases, animals are only subjected to abuse in order to produce content, whether pre-recorded or livestreamed, and therefore argued that "the very nature of the actions in the

[158] Crown Prosecution Service, 2024. 'Man jailed for posting videos of baby monkeys being tortured' [accessed 9 October 2024].
[159] Humane Society International response to August 2024 Further Consultation, p. 4. OSAN response to August 2024 Further Consultation, p. 5. RSPCA response to August 2024 Further Consultation, pp. 8-9. Scottish SPCA response to August 2024 Further Consultation on Torture and Animal Cruelty, pp. 7-8. Wildlife and Countryside Link response to August 2024 Further Consultation, p. 5.
[160] RSPCA response to August 2024 Further Consultation, p. 8.

content having been devised and filmed for another person to view and consume" means that such content amounts to offence of encouragement or conspiracy.[161]

2.364 For content to be illegal content, the content itself must 'amount' to the offence. Content amounts to an offence if: the use of the words, images, speech or sounds amounts to a relevant offence; the possession, viewing or accessing of the content constitutes a relevant offence; or the publication or dissemination of the content constitutes a relevant offence.[162] We accept that live acts are relatively rare, but we remain of the view that it is not legally possible to conspire to commit acts that have already happened. (Our argument regarding livestreaming relies upon the user committing the act of animal cruelty and the user viewing the acts both acting concurrently in a way which amounts to conspiracy).

2.365 With regard to encouragement, the inchoate offence of encouragement requires *intent* to encourage or *belief* that that or another offence will (not may) be committed. This means that, for content to amount to an offence, it must be *reasonable to infer* that, by posting the content concerned, the user posting intended to encourage or believed that another person would do an act amounting to an offence. Based on the evidence currently available to us, we do not consider that there are reasonable grounds to believe this. We do not dispute that harm caused to the animal, or that the dissemination of the content is to be deplored.

2.366 **Battersea Dogs and Cats Home** expressed concern drawing attention to the possibility of fantasising or joking "could too easily provide a defence for inaction on the part of service users or potential offenders that 'we thought they were joking,' which would be very difficult to disprove." However, intent to encourage, assist or conspire is a necessary part of the offence and a person who is joking is unlikely to have such intent. We have, however, made it clear that it is important for services to consider that "some users pretend something is a fantasy or a joke to disguise illegal content."

2.367 Further to the points raised by **Dogs Trust** in relation to ear cropping, and **Cats Protection** in relation to declawing, we acknowledge that 'how to' guides can encourage or assist this offence. We have therefore added wording explaining that content may be illegal where it provides practical instructions about how to commit the offence, and also added the following as usage examples: "Content providing instructions or advice on how to crop dog ears or declaw a cat."[163]

Online content and prosecutions under the AWA 2006 offence

2.368 Several respondents (**Born Free Foundation, RSPCA**, **Scottish SPCA**) highlighted cases where pre-recorded images and videos of animal cruelty were used to prosecute cases under the AWA 2006 offence.[164] However, the cases did not prosecute *the act of posting the content*. They used the content as proof of the offline animal cruelty, which was the conduct actually being prosecuted.

---

[161] SMACC response to August 2024 Further Consultation, pp. 4-5.
[162] Section 59(3) of the Act.
[163] Cats Protection response to the August 2024 Further Consultation on Torture and Animal Cruelty, p. 8. Dogs Trust response to August 2024 Further Consultation, p. 3.
[164] Born Free Foundation response to August 2024 Further Consultation, p. 5. RSPCA response to August 2024 Further Consultation, pp. 10-12. Scottish SPCA response to August 2024 Further Consultation, p. 8.

Use of the Animal Welfare (Sentencing) Act 2021 and animal cruelty content

2.369 In its response, the **Blue Cross** noted that the Animal Welfare (Sentencing) Act 2021 introduced new Sentencing Council guidelines ('Sentencing Guidelines') for the most serious animal cruelty offences, including the prosecution of section 4 of the AWA 2006 offence. These guidelines list the "use of technology, including circulating details/photographs/videos etc of the offence on social media, to record, publicise or promote cruelty" as an aggravating factor when determining the seriousness of the offence in question.[165] The Sentencing Guidelines do not create offences; they provide the framework for sentencing existing offences. This means they are not relevant in judgements about whether content amounts to an offence.

Approach to details of the s. 127(1) offence: use of phrase "no good reason"

2.370 In this section, we discuss the detail of our guidance relating to the s. 127(1) offence of sending (or causing to be sent), online, a message (or other matter) that is obscene, where the sender intended, or recognised, at the time of sending that it may be taken as obscene by a reasonable member of the public. For more high-level stakeholder responses and our decisions relating to the use of the s. 127(1) offence see paragraphs 2.62 to 2.69 and paragraphs A1.51 to A1.67 in the annex titled 'Annex to Volume 3'.

2.371 'Obscene' has no special legal definition. At consultation, we proposed that there would be reasonable grounds to infer that content is obscene where it "graphically depicts what appears to be the real: deliberate killing or serious injury of humans or animal for no good reason (*except* where such killing or serious injury is otherwise lawful, for example in war or food production); or torture of humans and/or animals.

2.372 **Battersea Dogs and Cats Home** and the **Humane Society International** both expressed concern about our use of the phrase "good reason."[166] **Humane Society International** described it as "quite subjective" and recommended that examples should be expanded.[167] **Battersea Dogs and Cats Home** similarly argued that "for no good reason" is "subjective and can be heavily influenced by an individual's ethical framework." It argued that "unlawful" would be clearer and easier to enforce than "for no good reason".[168]

2.373 We acknowledge the subjectivity inherent in the phrase "for no good reason" but believe that a focus on what is "lawful" is not appropriate as it would require service providers to have detailed knowledge of a broad swathe of UK legislation (including animal welfare legislation). We believe this is disproportionate to expect of service providers. We also believe it is impractical for Ofcom to provide such information. Given this limitation, we believe it is instead necessary to give clear examples of what is highly likely to be accepted by UK courts as obscene in this context.

2.374 We have therefore decided to amend the ICJG to state that content is obscene where it "graphically depicts what appears to be… the real and deliberate killing or serious injury of humans for the purposes of entertainment or amusement." We have provided two further usage examples to illustrate this point: "Content which graphically depicts the real and deliberate dismemberment of an animal or human where the dismemberment is carried

---

[165] Blue Cross response to August 2024 Further Consultation, p. 2.
[166] Humane Society International response to August 2024 Further Consultation, p. 5. Battersea Dogs and Cats Home response to August 2024 Further Consultation, p. 11.
[167] Humane Society International response to August 2024 Further Consultation, p. 5.
[168] Battersea Doogs and Cats Home response to August 2024 Further Consultation, p. 11

out for the purposes of entertainment" and "Content which graphically depicts severe injury of an animal in the course of dog fighting or hare coursing."

Approach to details of the s. 127(1) offence: exemption for food production

2.375 Several stakeholders, including **Google**, **Humane Society International** and **RSPCA** raised concerns about our inclusion of "typical food production" as an example of content that should not be considered obscene. The **RSPCA** argued that the proposed exemption is "subjective with regards to cultural norms of food production."[169] **Humane Society International** called the exemption "ambiguous."[170] **Google** noted that standards of food consumption vary across the world.[171]

2.376 We acknowledge the concerns raised but believe it is not appropriate to state that depictions of slaughter or killing in the course of typical food production (even where these are graphic) are to be considered obscene as it is too uncertain that UK courts would find this to be the case. Furthermore, we believe that any statement that such content is obscene would pose freedom of expression risks and would, in particular, risk over-takedown of content which is depicting food production for campaigning or educational purposes. We have therefore decided to retain our exemption for food production, although we have specified further that "typical food production" means activities "such as the breeding, rearing, keeping and slaughtering of chickens, cows, pigs, sheep and goats." We believe this clarification addresses the concern raised by Google about varying standards across the world, and captures the most common practices in the UK which are least likely to be considered 'obscene' by the UK courts.

Approach to details of the s. 127(1) offence: exemption for awareness-raising campaigns

2.377 Our August 2024 Further Consultation stated that where the depiction of severe injury or death "has a clear political or teaching objective, it is very unlikely that is illegal content" under the s. 127(1) offence. In its response, **Humane Society International** said that it did not consider that the proposed guidance offers sufficient clarity that it would not usually be reasonable to infer that content is obscene when it is posted in the course of campaigning for the protection of animals.[172] We acknowledge that further clarity could be given and have decided to update our guidance to clearly state that "it will *not* usually be reasonable to infer that content is obscene where it depicts… even in a graphic way and where the conduct shown is unlawful… an apparently real instance of cruelty (for example, demonstrations of cruelty in the keeping or breeding of animals) where the purpose is to educate or raise awareness about such cruelty." We believe this change to **Humane Society International**'s suggested wording broadens the scope of the exemption to include cruelty to people.

---

[169] RSPCA response to August 2024 Further Consultation, pp. 11-12.
[170] Humane Society International response to August 2024 Further Consultation, p. 4.
[171] Google YouTube response to August 2024 Further Consultation, p. 3.
[172] Humane Society International response August 2024 Further Consultation, p. 4.

3. Ofcom's enforcement powers

What is this chapter about?

This Chapter explains our general approach to regulatory enforcement, how we will approach enforcement under the Online Safety Act (the Act) and introduces our Online Safety Enforcement Guidance (the Guidance).

What decisions have we made?

We have retained the overall approach set out in our November 2023 Illegal Harms Consultation (the November 2023 Consultation) about how we intend to exercise our enforcement powers and have issued the Guidance alongside this Statement. Having considered respondents' comments on our draft Guidance we have made some minor changes, including to clarify how we intend to engage with affected stakeholders, and other entities with relevant expertise, before making an application for business disruption measures.

Why are we making these decisions?

Our approach to enforcement under the Online Safety Regime has been informed by our experience and track record of enforcement in other sectors we regulate. We believe it will enable us to take effective and timely enforcement action in the interests of citizens and consumers, including by driving compliance; protecting users, especially children, from harm; deterring future wrongdoing; and holding wrongdoers to account. The changes we have made provide further clarity for stakeholders on the process we will follow in doing so.

Introduction

3.1 The Act grants Ofcom a range of enforcement powers and requires us to produce guidance for service providers on how we will exercise them. The Online Safety Enforcement Guidance (the Guidance) sets out how we will normally approach enforcement under the Online Safety Act (the Act). The approach set out in the Guidance has been informed by our experience and long track record of enforcement work in the other sectors that we regulate.

3.2 We received 53 stakeholder responses relating to our approach to using our enforcement powers under the Act and the Guidance. The majority were broadly supportive of our proposals.

3.3 This chapter sets out:

a) our general approach to regulatory enforcement;
b) a summary of our approach to online safety enforcement, stakeholder responses to our November 2023 Illegal Harms Consultation and our decisions; and
c) what the Guidance covers, stakeholder responses to our November 2023 Consultation and our decisions.

3.4 Additional stakeholder comments received in response to our November 2023 Consultation are summarised and addressed in 'Annex 1 to the Statement on Further stakeholder responses'.

Our general approach to enforcement

3.5 The Communications Act 2003 (the Communications Act) requires Ofcom to have regard, in all cases, to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only in cases in which action is needed; and any other principles appearing to Ofcom to represent the best regulatory practice. In terms of enforcement, this means we will take action where it is proportionate and appropriate, with a willingness to intervene firmly, promptly and effectively when required. We will always seek the least intrusive regulatory methods to achieve our objectives and to ensure that interventions are evidence-based, proportionate, consistent, accountable, and transparent in both deliberation and outcome, in line with our regulatory principles.[173] These regulatory principles will also apply to online safety enforcement.

3.6 Ofcom uses a wide range of tools to encourage, promote and enforce compliance by regulated services with their regulatory obligations. These include:

a) supporting activities such as publishing guidelines, conducting research to better understand the markets that we regulate, and providing advice and education to consumers of communications services;
b) alternative tools that do not rely on legal powers, such as meetings or written communication with regulated services to discuss possible compliance issues and how they might be addressed through voluntary commitments; and
c) investigating breaches of regulatory rules using statutory enforcement powers set out in relevant legislation, which may lead to us issuing legally binding decisions on whether a regulatory breach has taken place, and which may impose financial penalties and other sanctions.

3.7 To help providers of services in scope of the Act navigate the new regulations and understand their obligations, we will also launch a new 'Digital Support Service', which will consist of interactive digital tools for regulated providers, based on their perspectives and feedback. These will not give specific compliance advice but are intended to make the requirements of the Act more accessible and attainable and to encourage service providers to consider what more they can do to ensure safe experiences for users.

Our approach to online safety enforcement

3.8 As the independent regulator for online safety in the UK, Ofcom will take enforcement action where it is in the interests of citizens and consumers to improve compliance, deter future wrongdoing, and protect users from harm, especially children. The Act sets out which of the duties imposed on providers of regulated services are subject to enforcement action by Ofcom.[174] As soon as each of these duties come into force, Ofcom may choose to use the relevant enforcement powers provided in the Act against any service provider that fails to comply with that duty.

3.9 In line with our proposals in our November 2023 Illegal Harms Consultation, our approach to enforcing compliance with the new duties as they start coming into force from December 2024 will be:

[173] See our Regulatory Principles.
[174] A table of enforceable duties is set out at section 131(2) of the Act.

- We expect all service providers to fully comply with duties that are currently in force, such as the duty to comply with Information Notices. Failure to do so means providers are at risk of enforcement action by Ofcom.
- We expect all service providers to comply with the illegal content risk assessment duties and children's access assessment and risk assessment duties by the statutory deadline. Failure to do so means providers are at risk of enforcement action by Ofcom. Specifically, providers of **all services** will need to:
  - **complete their first illegal harms risk assessments by mid-March 2025**, three months after the publication of our final guidance as part of this Statement;
  - **complete their first children's access assessments by mid-April 2025**, three months after the planned publication of our children's access assessment guidance in mid-January 2025; and
  - **complete their first children's risk assessments by the end of July 2025** if their service is likely to be accessed by children, three months after the planned publication of our children's risk assessment guidance at the end of April 2025.
- We have published our Illegal Harms Codes of Practice as part of this statement and plan to publish our Children's Codes of Practice in April 2025. The Codes of Practice will come into force 21 days after they complete their passage through Parliament. We expect the illegal harms safety duties to become enforceable around March 2025 and the child protection safety duties to become enforceable around July 2025.
- We acknowledge that it may take time for service providers to implement the necessary measures to bring themselves fully into compliance. We also acknowledge that some measures may take longer than others to implement. As such, for approximately the first six months following the duties coming into force, we will focus on ensuring service providers are adequately assessing risk and taking steps to put in place the measures that will be most effective at protecting users, especially children, from serious harms. After six months, we would expect almost all of the measures recommended in our Codes of Practice to be in place.
- However, we expect **all** service providers to start implementing appropriate measures **as soon as we issue the Codes of Practice following their passage through Parliament** in preparation for the duties coming into effect 21 days later. Early efforts should be focussed on putting in place mitigations that are most likely to protect users from the most serious harms, and we expect mitigations that are relatively quick or simple to implement to be completed rapidly.
- In addition, as soon as the duties come into effect, we will not hesitate to take enforcement action against deliberate or egregious breaches where there appears to be a very significant risk of serious and ongoing harm to UK users, and to children in particular. We will also launch broader multi-service or sector-wide compliance programmes where we believe there may be systemic issues that need swift and comprehensive action to achieve the necessary change.

Respondent comments

3.10 16 respondents commented on Ofcom's approach to online safety enforcement, which we summarise in this section.

3.11 Four respondents (including Airbnb, Google, Pinterest, and Protection Group International) said that six months is not long enough for service providers to ensure full compliance

ahead of the duties coming into force.[175] Airbnb said this period is too short to proactively engage with Ofcom if complex technical work is needed to comply with certain measures in the Codes of Practice. Google suggested that Ofcom should seek a period of up to 12 months for full compliance. Pinterest said that, depending on the relevant duty, six months may be a short turnaround to effectively plan, design, develop, test, and implement the required changes. Protection Group International suggested that we should allow a period of 12 months to include identifying new potential systems, testing, training, and certain costs. Another respondent, [✂], noted that providers of larger services will need time to transpose pre-existing systems, processes and controls, and for engineering changes, employee training, and dialogue with regulators.[176]

3.12 In contrast, Yoti said that allowing six months for providers to fully comply is unreasonable and runs contrary to the inclusion of the harm or risk of harm to children in the list of priority factors we consider before deciding whether to take enforcement action.[177] UK Finance also noted that there should be a cap on any case-by-case extensions to this to prevent service providers who delay updating their service controls being targeted by criminals.[178]

3.13 Four respondents asked for more clarity on timelines or a clearer roadmap for implementing the regime.[179] Ten respondents said that Ofcom should take further action to help service providers comply. The Association of Police and Crime Commissioners (APPC) suggested producing guidance.[180] The Local Government Association noted that Ofcom should engage with providers in the early months of the regime.[181] Others requested specific assistance for providers of small or low-risk services.[182] The Cyber Helpline suggested a 'buddy system' allowing smaller providers to be partnered up with larger service providers to help them be held accountable.[183]

Our decisions

3.14 As set out at paragraph 3.9, we expect providers of all services to implement appropriate measures as soon as possible, given the importance of mitigating any risk of harm to users, especially children and we expect them to start implementing the measures straightaway. However, we acknowledge that providers may need additional time to implement measures to achieve full compliance and that this might, in some instances, exceed the six-

[175] Airbnb response to November 2023 Illegal Harms Consultation, p.23; Google response to November 2023 Illegal Harms Consultation, p.75; Pinterest response to November 2023 Illegal Harms Consultation, pp.11-12; Protection Group International response to November 2023 Illegal Harms Consultation, p.15.
[176] [✂].
[177] Yoti response to November 2023 Illegal Harms Consultation, p.29.
[178] UK Finance response to November 2023 Illegal Harms Consultation, p.21.
[179] [✂]; DWF response to November 2023 Illegal Harms Consultation, p.1; Google response to November 2023 Consultation, p.75; Yoti response to November 2023 Consultation, p.28.
[180] APPC response to November 2023 Illegal Harms Consultation, p.4.
[181] Local Government Association response to November 2023 Illegal Harms Consultation, p.19.
[182] Federation of Communication Services response to November 2023 Illegal Harms Consultation p.1; Federation of Small Businesses response to November 2023 Illegal Harms Consultation, p.2; Global Partners Digital response to November 2023 Illegal Harms Consultation, p.23; Global Network Initiative response to November 2023 Illegal Harms Consultation p.8; IWF response to November 2023 Illegal Harms Consultation, pp.3-4; Oxford Disinformation Extremism Lab response to November 2023 Illegal Harms Consultation, p.20; Protection Group International response to November 2023 Consultation, p.13.
[183] The Cyber Helpline response to November 2023 Illegal Harms Consultation, p.21.

month period we are generally allowing for measures to be fully in place; for example, where there are technical complexities in modifying existing systems and processes.

3.15 We will consider what is reasonable on a case-by-case basis when deciding whether to take enforcement action during the period immediately following the duties coming into force and will take into account the actions being taken to implement the necessary measures and achieve full compliance. However, from the outset we will not hesitate to take action against serious breaches where there appears to be a very significant risk of harm to UK users, and to children in particular. Early efforts should therefore be focussed on putting in place mitigations that are most likely to protect users from serious potential harms, and measures that are relatively quick or simple to implement should be completed rapidly.

3.16 If service providers are concerned about their ability to comply, we encourage them to engage with Ofcom at an early stage, which may enable us to resolve issues using tools other than enforcement. However, we expect service providers to have already started preparing for the duties coming into force and we have regularly published information on our website to help them understand how they can do so.[184]

3.17 We acknowledge that smaller service providers may need additional support to come into compliance with their duties under the Act. We have been engaging with service providers, particularly providers of smaller services, to help them understand the new rules, and we are publishing guidance in a range of areas. We are developing a Digital Support Service to make the requirements more accessible and attainable. We have also produced materials, including a series of webinars, to help service providers understand and engage in the consultation process for the Codes of Practice.[185] On 17 October 2024 we published a progress update on our implementation of the regime, which makes clear what providers need to do to comply with the rules as they start to come into force from December 2024.[186]

Online Safety Enforcement Guidance

3.18 We have today published standalone Guidance so that there is clarity for providers of newly regulated services about our enforcement procedures under the Act. This is available on the Ofcom website.[187] We have published a separate consultation on our proposed guidance on how we will use our information gathering powers.[188] Our final guidance will be published in early 2025.

3.19 The Guidance is divided into 10 sections:

1) Overview
2) Introduction
3) Enforcement action and when we use it
4) Initial assessment of the issues
5) Opening an investigation and information gathering

[184] For example see our publication: New rules for online services: what you need to know, 27 February 2024.
[185] See our Webinar: Introduction to the Online Safety Act and the illegal harms consultation.
[186] See our October 2024 update: Implementing the Online Safety Act: progress update (ofcom.org.uk).
[187] Link to Online Safety Enforcement Guidance
[188] Consultation on Online Safety Information Guidance, 26 July 2024. The stakeholder responses to Chapter 28 of the November 2023 Consultation which set out Ofcom's approach to its Online Safety Information Gathering Powers are summarised in this separate Consultation.

6) Determining the outcome of our investigation
7) Liability of Related Entities and Controlling Individuals
8) Settlement procedure
9) Business disruption measures
10) Procedural complaints about investigations

3.20 In the next section we summarise the areas of the Guidance that stakeholders responded to as part of our November 2023 Consultation, and our decisions.

Enforcement action and when we will use it

3.21 This section of the Guidance focuses on how and when Ofcom may decide to take enforcement action. It sets out our principal duties and objectives, as well as other matters to which we must have regard. It lists the priority factors we will consider when making decisions about whether to take enforcement action (the "priority framework"). It also explains some of the ways in which Ofcom may become aware of potential compliance issues and the range of enforcement tools that we might consider in response to these issues, including non-statutory alternative enforcement tools.

Respondent comments: how Ofcom becomes aware of compliance issues

3.22 We received five responses about Ofcom's approach to identifying potential compliance issues: four respondents recommended that Ofcom take a more proactive approach to identifying non-compliance under the regime, rather than assuming service providers will comply with the requirements.[189] [✂].

Our decisions

3.23 We have decided to maintain the approach set out in the November consultation. Decisions about whether to take enforcement action are made on a case-by-case basis, having regard to our statutory duties and all the matters that appear to be relevant, including the priority factors set out in paragraph 3.9 of the Guidance.

3.24 We use a wide range of tools to promote compliance in addition to our statutory enforcement powers, as set out in paragraphs 3.11 to 3.15 of the Guidance. We identify potential compliance issues through a range of sources, as set out in paragraph 3.5. This includes information that may be provided to us by other regulatory bodies or enforcement agencies and matters that may have come to our attention through our engagement with supervised services.[190] Under the Act, systemic issues can be reported to Ofcom by eligible entities as super-complaints.[191] Individual complaints can also be flagged or reported to Ofcom's Consumer Contact Team or through our online safety complaints portal.[192] While we do not respond to individual complaints, we monitor trends to identify where there may be systemic issues. We have developed tools to help us identify the areas with the greatest

[189] [✂]; Domestic Abuse Commissioner's Office response to November 2023 Illegal Harms Consultation, pp.6-7; Phoenix 11 response to November 2023 Illegal Harms Consultation, p.3; Suzy Lamplugh Trust response to November 2023 Illegal Harms Consultation 2023, p.7; Yoti response to November 2023 Consultation, pp.27-29.
[190] For example, the Information Commissioners Office (ICO), National Crime Agency (NCA), or the Advertising Standards Authority (ASA).
[191] Ofcom will consult on and publish guidance around super-complaints in 2025, including information on how an entity can verify its eligibility against the criteria and the procedures for making a super-complaint.
[192] Ofcom complaints portal: online services, websites or apps.

risk of harm to users and will proactively monitor compliance in high-risk areas through multi-service or sector-wide compliance programmes.

Respondent comments: enforcement action and when we use it

3.25 Four respondents commented on the need for Ofcom to take prompt and effective enforcement action.[193] The APPC said it was concerned that we state that we "may" take certain action and noted that "cases with automatic enforcement are needed to ensure the most effective safeguarding against criminal behaviours". The Institute for Strategic Dialogue (ISD) said that, in relation to non-compliant providers of small services posing a severe risk, swift action would assist other providers of smaller services to understand their obligations. Yoti disagreed with Ofcom's regulatory principle of bias against intervention, stating that this should be changed to "we operate with a preference for softer regulatory interventions initially, but nevertheless, a willingness to intervene promptly and effectively when required".

Our decisions

3.26 We expect to prioritise enforcement for the most harmful cases, in line with our priority framework as set out in paragraph 3.9 of the Guidance. It is not possible for Ofcom to investigate every potential compliance issue that arises in relation to each enforceable duty in the Act. Therefore, as we set out in the Guidance, it is important that we maintain discretion about when to take action, so that we do so in an efficient and effective way, in accordance with our regulatory principles.

3.27 The priority framework already takes into consideration both the risk of harm and the strategic significance of addressing any alleged contravention, which includes clarifying the regulatory or legal framework for other stakeholders. Further, as set out in the Guidance, we may open enforcement programmes where we consider there is an industry-wide issue which is causing harm.[194] Our central objective when imposing a penalty is deterrence, both to deter the regulated body subject to the penalty from further misconduct, and to provide signals to the wider industry that are sufficient to incentivise them to comply. This is set out in our Penalty Guidelines.[195] Accordingly, we consider that our approach to enforcement is already designed to ensure that action we take assists the wider industry to understand their obligations under the Act.

3.28 We have removed the wording in the draft Guidance that we operate with a bias against intervention, in light of respondents' comments. We refer to the statutory language in respect of our duty 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 principles appearing to Ofcom to represent best regulatory practice.[196] We have made clear that, in terms of enforcement action, our approach is to take action only where it is proportionate and appropriate, but with a willingness to intervene firmly, promptly and effectively when required.

---

[193] APPC response to November 2023 Consultation, p.7; Blue Cross response to the August 2024 Illegal Harms Further Consultation on Torture and Animal Cruelty, p.8; ISD response to November 2023 Illegal Harms Consultation, p.18; Yoti response to November 2023 Consultation, p.27.
[194] See the Online Safety Enforcement Guidance, paragraph 3.13.
[195] Ofcom: Penalty Guidelines as amended.
[196] Section 3(3) of the Communications Act 2003.

Respondent comments: priority framework

3.29 Five respondents commented on the factors set out in the priority framework, which we summarise in this section. Three respondents commented on the importance of prioritising child safety: the Children's Commissioner and the Local Government Association said that Ofcom should enforce compliance with children's safety duties robustly and swiftly to minimise harm; Glitch said that more detailed guidance could be provided on how child safety considerations will be integrated into enforcement decisions. [197]

3.30 Two respondents commented on Ofcom's use of its enforcement powers and the potential effect on user rights: Christchurch Call Advisory Network expressed concern that some of the enforcement provisions, if used too extensively, could result in service providers taking sweeping measures to comply with the Act that do not sufficiently consider the effect on users' rights; British and Irish Law, Education and Technology Association (BILETA) stated that the existing priority framework does not ensure that proportionality will be exercised in cases where user rights are significantly affected by enforcement action.[198]

3.31 Google disagreed with one factor we listed as an example of what we may consider when thinking about the strategic significance of addressing the alleged contravention, namely whether enforcement action would help clarify the regulatory or legal framework for other stakeholders, found in paragraph 3.9 b) i) of the Guidance.[199] Google stated that enforcement should not be used to clarify ambiguity in the Codes of Practice and suggested adding to the priority framework consideration as to whether a provider self-reported or otherwise voluntarily notified Ofcom of an issue.

3.32 One respondent asked if enforcement action is likely to be limited in cases dealing with retrospective harm.[200]

3.33 Glitch suggested that the priority framework could be strengthened by providing specific guidance on how each of the priority factors will be weighed and how this might affect marginalised groups negatively.[201]

Our decisions

3.34 Securing a higher level of protection online for children than adults is one of the objectives of the Act. The Act also requires that the Guidance includes an explanation of how we will take account of the effect (or possible effect) of non-compliance on children. As such, the harm, or risk of harm to children, is included in the priority framework set out in paragraph 3.9 of the Guidance. This will be taken into account by Ofcom both when considering the risk of harm or seriousness of the conduct and the strategic significance of addressing the alleged contravention. As such, we consider that our approach adequately ensures the prioritisation of protection of children.

3.35 We acknowledge Christchurch Call Advisory Network and BILETA's concerns around the effect of our enforcement action on user rights. In view of the context in which these

[197] Children's Commissioner response to November 2023 Illegal Harms Consultation, p.23; Local Government Association response to November 2023 Consultation, p.19; Glitch response to November 2023 Illegal Harms Consultation, p.13.
[198] Christchurch Call Advisory Network response to November 2023 Illegal Harms Consultation, p.4; BILETA response to November 2023 Illegal Harms Consultation, p.24.
[199] Google response to November 2023 Consultation, pp.75-76.
[200] [✂].
[201] Glitch response to November 2023 Consultation, p.13.

comments were made, we understand the focus of the respondents' concern to be the potential effect that enforcement action may have on rights to freedom of expression under Article 10 of the European Convention on Human Rights (ECHR).[202] As a public body, it is unlawful for Ofcom to act in a way that is incompatible with the rights set out under the ECHR (Convention rights).[203] Therefore, when considering or taking enforcement action, we will take into account the potential effects on freedom of expression when deciding how to proceed. This is separate to the application of the priority framework, which is intended to ensure that we use our enforcement resources in an efficient and effective way.

3.36 In response to Google's point that enforcement should not be used to clarify ambiguity in the Codes of Practice, we disagree. The Codes of Practice are not able to anticipate every possible scenario, so it is not possible to exclude the potential for ambiguity to emerge. Our enforcement practice may be used to provide clarity in such circumstances, and it is standard regulatory practice for this to be considered as a potentially relevant factor when deciding whether to take enforcement action.[204] This is also a factor in our Regulatory Enforcement Guidelines.[205]

3.37 On Google's separate suggestion that the priority framework should be amended to take into account whether a service provider has self-reported an issue, we encourage providers to report issues to Ofcom and to act transparently. However, evaluating the seriousness of a potential issue with a service is independent of the way it was reported to us or brought to Ofcom's attention. Should we decide to impose a penalty, self-reporting may be a mitigating factor we consider when determining the amount, in line with our Penalty Guidelines.[206]

3.38 In response to the comments on retrospective harm, Ofcom may take enforcement action where we have concerns that a provider has failed or is failing to comply with its duties under the Act. The fact that the harm is retrospective, or the non-compliant conduct has ceased, does not in itself mean that Ofcom is unlikely to take action. We consider each of the factors set out in the priority framework when deciding whether to take action in each case.

3.39 In response to Glitch's comment on how each of the priority factors are weighed, we consider that the level of detail included in the priority framework is sufficient. This is because issues are assessed on a case-by-case basis and factors will be weighed depending on the individual circumstances of each case.

Respondent comments: Ofcom's enforcement and compliance tools

3.40 One respondent suggested Ofcom clarify whether the alternative compliance tools in paragraph 3.13 of the Guidance could be used in parallel with opening an investigation.[207]

---

[202] The European Convention on Human Rights [accessed 28 November 2024].
[203] Section 6, Human Rights Act 1998.
[204] For example, similar factors are included in the Competition and Markets Authority's Prioritisation Principles [accessed 28 November 2024]; the Payment System Regulator's Administrative Priority Framework [accessed 28 November 2024]; and the Information Commissioner's Office's Regulatory Action Policy [accessed 28 November 2024].
[205] See our Regulatory Enforcement Guidelines for investigations.
[206] Ofcom: Penalty Guidelines as amended.
[207] [✂].

Our decisions

3.41 Ofcom cannot open investigations into every potential compliance issue that arises in relation to each enforceable duty in the Act. It is important that we use our discretion to take action in an efficient and effective way, in accordance with our regulatory principles. As part of this, we will use other tools, such as warning letters or compliance remediation, where we consider that they can effectively and efficiently address compliance concerns that we have identified. As we explain in paragraph 3.13 of our Guidance, remediation may include a period of compliance monitoring to ensure the service provider does not repeat behaviour that led to the issues in the first place. Should further concerns arise, we will consider what action to take, which may include an investigation.

3.42 As noted above, we may open enforcement programmes where we consider there is an industry-wide issue which is causing harm. We may open one or more investigations if specific compliance concerns by a particular provider or providers come to light in the course of an enforcement programme.

Initial assessment of the issues

3.43 This section of the Guidance explains what an initial assessment is and how we engage with service providers during the process of carrying out an initial assessment. It also sets out the potential outcomes of an initial assessment.

Respondent comments: engagement with service providers during the initial assessment

3.44 One respondent asked whether the list of reasons given in paragraph 4.14 of the Guidance, for Ofcom not to inform a service provider that it is carrying out an initial assessment, are exhaustive.[208]

Our decisions

3.45 The examples set out in paragraph 4.14 of the Guidance, of circumstances where we may decide not to engage with a service provider during our initial assessment, are not exhaustive. We would be unlikely to engage with a provider at this stage if we had information suggesting it would act in a manner detrimental to the enforcement process.

Respondent comments: potential outcomes of an initial assessment

3.46 One respondent asked for additional information around the actions listed in paragraph 4.16 of the Guidance and whether they could preclude a formal investigation.[209]

Our decisions

3.47 Paragraph 4.16 of the Guidance sets out that, where appropriate, Ofcom may consider whether other action is suitable after conducting an initial assessment. Namely, whether to apply to court for a Business Disruption Order, issue a Notice to deal with terrorism and child sexual exploitation and abuse content (Technology Notice), or require a skilled person's report.

3.48 To make an application for a Business Disruption Order we would need sufficient evidence that the relevant statutory tests for making such an application to the court have been met.

---

[208] [✂].
[209] [✂].

In most cases, we would expect to gather such evidence as part of a formal investigation. However, there may be cases where sufficient evidence has come to light during the initial assessment that would prompt us to make an application before opening a formal investigation. In respect of issuing a Technology Notice, Ofcom can issue a Notice without opening a formal investigation. However, if the service provider fails to comply this is likely to lead to a separate investigation to enforce their duty to comply with such a notice.[210] The power to require a skilled person's report is an information gathering tool which we may use to gather further information to help us determine whether an investigation is warranted.[211] It may also be used in the course of an investigation to support our assessment of a provider's compliance with their duties.

Respondent comments: confidentiality at initial assessment stage

3.49 Google said that Ofcom should make clear that information provided by a service provider voluntarily at initial assessment stage, which is not given in response to a request under Ofcom's information gathering powers (in line with paragraph 4.12 of the Guidance), will be treated as confidential and not shared with third parties. It also said that, where service providers are given advance notice of the publication of information relating to enforcement proceedings, Ofcom should allow sufficient time for the provider to make representations on confidentiality. It suggested five working days as an appropriate time period.[212]

Our decisions

3.50 Section 393(1) of the Communications Act prohibits the disclosure of information which relates to a business which Ofcom has obtained as a result of its powers under the Online Safety Act. However, this prohibition is subject to the gateways in section 393(2) of the Communications Act, which enable the disclosure of such information in certain circumstances. These include a disclosure which Ofcom makes for the purposes of carrying out its functions. Information covered by the disclosure provisions of section 393 includes information relating to a business which we have obtained using our information gathering powers and information provided voluntarily by a service provider. For example, during an initial assessment, or at any other stage of the enforcement process.

3.51 There may be situations where it is necessary to disclose information in the course of an initial assessment or an investigation to facilitate the exercise of our functions. We also have duties to publish certain information, such as a confirmation decision.[213] For this reason, it is important that where a service provider gives information to Ofcom that they consider to be confidential, it should be clearly identified as such, along with the reasons why. We are mindful of the importance of protecting confidential information and will generally redact it when making a disclosure. If we consider that it may be necessary to disclose information identified as confidential for the purposes of carrying out our functions, we will inform the service provider in question and provide a reasonable

[210] Further information is set out in Ofcom's 16 December 2024 Consultation: Draft Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Act.
[211] Further information on the use of these powers is set out in Ofcom's 26 July 2024 Consultation on our proposed Online Safety Information Guidance. Our final guidance will be published in early 2025.
[212] Google response to November 2023 Consultation, p.77.
[213] Section 149 of the Act.

opportunity for it to make representations before making a final decision on whether to do so.[214]

3.52 When we publish information about our enforcement action, in accordance with our duty under section 149 of the Act, we must not include information which we consider to be confidential. [215] Prior to publishing information about enforcement action on Ofcom's website we will usually notify service providers no more than one working day in advance and provide a copy of the intended text for information only. This is in line with paragraphs 4.24, 4.29, 5.19 and 8.29 of our Guidance.

Opening an investigation and information gathering

3.53 In this section of the Guidance, we explain the purpose of an investigation, the process Ofcom will generally take following a decision to open an investigation, and our approach to information gathering. We also explain when we will generally publish details of investigations and again cover how we treat confidential information.

Respondent comments: engagement with complainants

3.54 Meta said in response to the November 2023 Consultation that the level of engagement with complainants set out in the Guidance goes beyond what would be typical in other regulatory contexts. Meta added that it would not be appropriate to provide regular updates about investigations to any third parties, including complainants.[216]

Our decisions

3.55 The Guidance sets out Ofcom's usual process for engaging with complainants where we have decided that it is appropriate to do so for reasons of fairness and transparency. The Guidance explains that we will decide on whether and when it is appropriate to do so on a case-by-case basis, depending on the nature of the investigation.[217]

Respondent comments: evidence

3.56 Two respondents provided comments on the evidence we might gather as part of our enforcement work. One respondent asked Ofcom to define what it means by "evidence" in the Guidance.[218] Meta sought clarification and examples on what kind of evidence would be required for an investigation to be triggered. It added that the evidential bar should be high, especially given Ofcom's intention to publicise the opening of an investigation.[219]

Our decisions

3.57 We do not consider it necessary to define what is referred to as evidence in the Guidance. Any information gathered through our enforcement processes might inform our decision to open an investigation and be included in our evidence base for any decision we may reach as part of our investigation. In relation to Meta's query around the evidential bar for triggering an investigation, the Act does not set an evidential threshold. However, we must act in accordance with our general duties including our duty to have regard to the

[214] Please refer to paragraphs 5.45 to 5.50 of the Guidance and our Draft Online Safety Information Powers Guidance for more information.
[215] Section 149(3) of the Act.
[216] Meta response to November 2023 Illegal Harms Consultation, pp.44-45.
[217] We make reference to this in 5.24 of the Guidance.
[218] [✂].
[219] Meta response to November 2023 Consultation, p.44.

regulatory principle that regulatory activities should be targeted only at cases where action is needed. When deciding whether to open an investigation, we will consider whether the evidence warrants it, as well as assessing the case against the factors set out in the priority framework (set out in paragraph 3.9 of the Guidance).

Respondent comments: publishing information about investigations

3.58 Five respondents provided comments on the importance of transparency in the enforcement of online safety duties.[220] Oxford Disinformation and Extremism Lab urged the creation of more robust and responsive oversight of Ofcom's enforcement powers and Guidance from elected officials, civil society, and academia. It suggested this could take the form of a permanent and independent advisory council or a pre-existing body.[221] UK Finance said that publicly reporting enforcement action and outcomes, similar to the Financial Ombudsman Service and Financial Services regulators (including the Bank of England, Financial Conduct Authority, and Prudential Regulation Authority) could deter online service providers and ensure there is an incentive to take steps to prevent harmful content from appearing.[222]

3.59 Yoti said it would like a stronger commitment from Ofcom on transparency and consistency, to drive trust in citizens and consumers relying on effective enforcement of the Act. It said Ofcom should provide more detailed information and make firmer commitments around the time taken at each stage of the enforcement process, including providing transparency around requiring steps to be taken. It said Ofcom should publish provisional notices of contraventions and confirmation decisions to be more transparent and foster trust. It said this would also enable providers to better assess which mitigation measures Ofcom deems sufficient or not and therefore increase the likelihood of compliance.[223]

3.60 Meta asked Ofcom to reconsider the approach set out in paragraph 5.14 of the Guidance around publishing information about the commencement of every investigation alongside regular updates. It said this approach was disproportionate and carried the risk of creating expectations around the outcome of the investigations, putting pressure on Ofcom to resolve cases prematurely and setting Ofcom up for public dissatisfaction. It said this could also negatively and unfairly affect the subject of the investigation as well as encourage parallel litigation. It suggested that Ofcom only publicise information relating to an investigation at the stage where it has taken the decision to issue a confirmation decision or a penalty notice. Meta also said that investigation milestones should only be published where there are exceptional circumstances to justify it. It said this would align with the approach of other regulatory regimes.[224]

Our decisions

3.61 We disagree with Meta's comments on our approach to publishing investigation updates and milestones. In line with our regulatory principles of transparency and accountability, we consider that it is appropriate to publish information about our investigations. As set out in the Guidance, this will typically include a case opening announcement and updates at

[220] Global Partners Digital response to November 2023 Consultation, p.26; Children's Commissioner response to November 2023 Consultation, p.23; SWGfL response to November 2023 Illegal Harms Consultation, p.16.
[221] Oxford Disinformation and Extremism Lab response to November 2023 Consultation, p.24.
[222] UK Finance response to November 2023 Consultation, p.21.
[223] Yoti response to November 2023 Consultation, p.29.
[224] Meta response to November 2023 Consultation, pp.46-47.

important milestones. These publications do not indicate that a decision has been made around whether there has been a breach of an enforceable requirement. A final decision will only be reached once our investigative process has concluded. Where we find a breach, we will publish a non-confidential version of the confirmation decision, including any remedial steps required. We therefore consider that our enforcement procedures provide for an appropriate level of transparency, which is in line with the suggestions made by other respondents.

3.62 We aim to carry out investigations and other enforcement activity as quickly and efficiently as possible. However, the length of time needed to complete an investigation will depend on the individual circumstances of each case, so we do not consider it appropriate to set specific timescales.

3.63 As set out in paragraph 5.21 of the Guidance, there may be exceptional circumstances in which we consider it would be inappropriate to publish details of an investigation, for example where a case has particular sensitivities or where publicity could have a detrimental effect on third parties. This will be assessed on a case-by-case basis.

Respondent comments: confidentiality during an investigation

3.64 Meta said that it disagreed with the requirement, set out in paragraph 5.47 of the Guidance, that service providers providing information that they consider to be confidential during an investigation should clearly identify it as such, including why it is confidential.[225] It said that Ofcom's Guidance should reflect the statutory requirement set out in section 393 of the Communications Act that all information provided by service providers pursuant to the exercise of Ofcom's powers under the Act is deemed confidential unless a service provider expressly confirms otherwise.[226]

Our decisions

3.65 We disagree with Meta's assertion that all information provided by service providers is automatically confidential under section 393 of the Communications Act unless the provider confirms otherwise. In fact, section 393 of the Communications Act imposes a general restriction on the disclosure of **any** information which relates to a business and which has been obtained in the exercise of Ofcom's powers, including those under the Act, unless the person carrying on the business in question consents to the disclosure. This general restriction is subject to the gateways for disclosure in section 393(2) which set out circumstances when disclosure without consent is permitted. These include a disclosure which is made for the purpose of facilitating the carrying out by Ofcom of any of its relevant functions, including enforcing the requirements of the Act.

3.66 Where we are considering whether to make a disclosure in accordance with section 393(2) of the Communications Act or publish information for the purposes of carrying out our functions, we will always consider whether redactions are required in respect of confidential information. Service providers are better placed than Ofcom to identify information which they consider to be detrimental to their business interests. For this

[225] Meta response to November 2023 Consultation, p.47.

[226] Section 393(1) of the Communications Act 2003 states that "… information with respect to a particular business which has been obtained in exercise of a power conferred by… the Online Safety Act 2023 is not, so long as that business continues to be carried on, to be disclosed without the consent of the person for the time being carrying on that business".

reason, it is important that those providing information to Ofcom clearly identify anything considered as confidential, alongside the reasons for this.

Determining the outcome of a compliance investigation

3.67 This section of the Guidance explains how Ofcom decides on the outcome of a compliance investigation and who makes the main decisions. It also sets out the stages of our process, from deciding whether to issue a provisional notice of contravention, to deciding whether to issue a confirmation decision on whether there has been a contravention.

Respondent comments: representations during an investigation

3.68 One respondent asked whether a service provider could make representations at any point during an investigation.[227]

Our decisions

3.69 Ofcom will engage with service providers throughout the investigative process and keep them updated on progress. Providers are able to make written submissions as they choose. In addition, it is a requirement of the Act that a recipient of a provisional notice of contravention is given the opportunity to make representations about the matters set out in the notice. The Guidance reflects this legal requirement in paragraphs 5.4 and 6.3. This standardised process ensures that the subjects of our investigations are treated fairly and consistently.

Respondent comments: closing an investigation following a provisional notice of contravention

3.70 One respondent said it would be helpful for Ofcom to clarify in paragraph 6.8 of the Guidance whether it expects to close an investigation in all cases where the non-compliant conduct ceases.[228]

Our decisions

3.71 Paragraph 6.8 of the Guidance states that we may decide to close an investigation either prior to, or following, a provisional notice of contravention being issued and that one of the reasons we may choose to do so is if we are satisfied the conduct has ceased, such that continuing the investigation no longer constitutes an administrative priority. However, while all relevant factors will be taken into account, in most cases simply ceasing the non-compliant conduct would not be enough for us to take the decision to close a case following the issuing of a provisional notice of contravention.

Respondent comments: re-opening an investigation

3.72 One respondent asked Ofcom to clarify the circumstances in which an investigation could be re-opened.[229]

Our decisions

3.73 Paragraph 4.26 of the Guidance makes clear that, where Ofcom has attempted to resolve a compliance issue through means other than formal investigation, it may revisit that decision where we become aware of further issues relating to the same or a similar issue, or

[227] [✂].
[228] [✂].
[229] [✂].

where such alternative means have not successfully resolved the issue. We consider that the position proposed in the November 2023 consultation is sufficiently clear.

Respondent comments: financial penalties

3.74 Four respondents sought clarification on Ofcom's approach to financial penalties. The Center for Data Innovation (CDI) said the Guidance should be clearer about when Ofcom will impose penalties, as there is a threat of increased censorship and moderation if Ofcom penalises service providers for not taking content which it deems illegal down swiftly enough. It said over-enforcement of the rules could negatively affect freedom of expression and that Ofcom should expand on what it deems appropriate and proportionate when it comes to issuing penalties.[230] One respondent asked about the minimum financial penalty Ofcom would impose and how this would be determined.[231] Google asked Ofcom to clarify when financial penalties will be imposed following the issue of a confirmation decision. It said it expects that any penalty, including daily penalties, would not be payable until the deadline for appealing the confirmation decision has expired or after the outcome of any appeal.[232] Revolut said that Ofcom should consider the rates of fraud carried out on a service when determining the level of penalty to impose.[233]

Our decisions

3.75 In response to the CDI's comment, as we explain at paragraph 3.6 of the Guidance, the objective of the Online Safety Regime is to regulate service providers' safety systems and processes, not individual pieces of content found on such services. The presence of illegal content, or content that is potentially harmful to children, does not necessarily mean that a service provider is failing to fulfil its duties in the Act. We would not, therefore, be likely to take action solely based on a piece of content appearing on a regulated service. However, we have also set out in paragraph 3.6 circumstances which might result in action being taken; for example, evidence of especially harmful material (particularly if it is on a service for a prolonged period without being removed), or a prevalence of harmful material (particularly where this is present on a service that presents a particular risk to children). We make decisions about whether to open an investigation on a case-by-case basis, having regard to our statutory duties and all the matters that appear to be relevant. As a public authority, our duties include our obligations under section 6 of the Human Rights Act 1998, to act in a way that is compatible with Convention rights, including the right to freedom of expression.

3.76 The decision to impose a penalty where we find a breach, and the amount of the penalty imposed, is also assessed on a case-by-case basis, in line with our Penalty Guidelines.[234] We consider all the circumstances in the round, taking account of relevant factors, such as those set out in our Penalty Guidelines. These include the degree of harm, whether actual or potential, resulting from the contravention. Therefore, where the contravention has resulted in fraud being carried on the service in question, this would be considered in our assessment. When we set a penalty, we are required to act in a way that is compatible with Convention rights, including the right to freedom of expression.

---

[230] CDI response to November 2023 Illegal Harms Consultation, p.21.
[231] [✂].
[232] Google response to November 2023 Consultation, pp.77-78.
[233] Revolut response to November 2023 Illegal Harms Consultation, p.22.
[234] Ofcom: Penalty Guidelines as amended.

3.77 Since all penalties are decided on a case-by-case basis, we do not have a minimum penalty. Our central objective when imposing a penalty is deterrence. Therefore, to ensure that any penalty we set has an appropriate deterrent effect, we take into account the size and economic strength of the service provider in question. The period in which a penalty must be paid by the service provider will be set out in the confirmation decision. The payment of a penalty is not automatically suspended pending the outcome of an appeal, but it is open to the applicant to seek Ofcom's consent to such a suspension.

Liability of Related Companies and Controlling Individuals

3.78 In certain situations, Ofcom may issue a provisional notice of contravention or a confirmation decision to both the service provider and another entity related to the service that is the subject of the contravention. Where we do so, the related entity will be jointly and severally liable for any contravention of that service that we find in a confirmation decision. In this section of the Guidance, we explain which entities may be issued with a notice jointly with the service provider under the Act, and the factors we will take into account when deciding whether this might be appropriate. We also explain how our enforcement procedures apply in these situations.

Respondent comments: Related Companies and Controlling Individuals

3.79 Google submitted that the Guidance does not reflect that a relevant decision or notice may only be given to a subsidiary under the Act where it contributed to the failure in respect of which the decision or notice is given. It also stated that paragraphs 7.15 to 7.20 of the Guidance suggest that Ofcom may also consider it appropriate to pursue a Related Company, including subsidiaries, where enforcement action would be more effective if taken against the Related Company as well as the service provider; for example where a service provider is based overseas and Ofcom has concerns about the resource required to ensure compliance with any confirmation decision. Google argued that this went further than the requirements of the Act and noted that under the Act, and in English law more generally, subsidiaries are not held liable for the actions of parent companies, unless they have been materially culpable in the infringing conduct, and particularly where the basis for doing so is primarily due to perceived inefficiencies when enforcing overseas.[235]

3.80 It also referred to paragraph 7.24 of the Guidance, which states that the relevant qualifying worldwide revenue consists of the (i) service provider, and (ii) every other company that is in the same company group as the service provider. It suggested we clarify that the "same company group" refers to "group undertaking" as defined in section 1161(5) of the Companies Act 2006.[236]

Our decisions

3.81 As explained at paragraphs 7.9 and 7.11 of the Guidance, a subsidiary which qualifies as a subsidiary undertaking or fellow subsidiary entity in relation to a service provider may only be held jointly and severally liable for a breach if the acts of the subsidiary contributed to the failure or contravention in question. Even where a subsidiary meets these requirements, Ofcom has discretion as to whether to seek to hold the subsidiary jointly and severally liable. We have set out at paragraphs 7.15 to 7.20 of the Guidance factors we may consider when deciding how to exercise our discretion. These do not alter the requirements

[235] Google response to November 2023 Consultation, pp.74-75.
[236] Google response to November 2023 Consultation, p.78; Companies Act 2006 (legislation.gov.uk).

that must be satisfied under the Act to hold a subsidiary jointly and severally liable for a contravention.

3.82 We have replaced references in Section 7 of the Guidance to a "company" with "undertaking" to align with the statutory language in Schedule 15 of the Act, in light of Google's comments.

Settlement procedure

3.83 In some cases, Ofcom may consider that it is appropriate to settle an investigation. In this section of the Guidance, we explain the minimum requirements for settlement and the discounts that Ofcom may apply to any penalty that is imposed when settlement is reached.

Respondent comments

3.84 Two respondents (Google and Meta) questioned why Ofcom considers it appropriate to depart from the principle of conducting settlement on a 'without prejudice' basis, such as occurs between parties to litigation or potential litigation, as set out in paragraph 8.33 of the Guidance.[237] They said the principle was necessary to prevent any admissions made during the settlement process being used against the service provider in subsequent proceedings if a settlement is not reached, and that this approach was likely to deter service providers from settling. Google added that additional documentary evidence provided during the process should not be made available to the final decision maker for the outcome of the regulatory process if the settlement was unsuccessful.

3.85 Meta also said that the maximum settlement discount of 30% should be available for all settlements agreed prior to Ofcom issuing a confirmation decision, if the provider agrees to the terms of the provisional notice of contravention within a specified timeframe. It said that this was akin to the approach adopted by the Financial Conduct Authority (FCA) and would encourage settlement and an effective and efficient resolution to the enforcement process. Meta also disagreed with the approach set out in paragraph 8.17 that it is unlikely to be appropriate to pursue settlement if a subject of the investigation is not prepared to agree to a settlement based on the statement of facts prepared by Ofcom. It said this differs from the approach taken by other regulators and that a core part of the settlement process should be Ofcom and the service provider working together to agree the statement of facts. Additionally, Meta said that the settlement decision maker should be independent to the case team, removing any perception of unfairness.

Our decisions

3.86 As set out in paragraph 8.3 of the Guidance, Ofcom's settlement process is not a negotiation and is not comparable to a commercial litigation process. It is a voluntary process in which the subject of an investigation participates of its own volition. There is no obligation for service providers subject to an investigation to agree to the terms of settlement offered by Ofcom. Paragraphs 8.31 and 8.32 make clear that if the settlement process is unsuccessful the investigation will revert to the usual process. Accordingly, if the provider is unable to agree the statement of facts prepared by Ofcom, subject to representations on manifest factual inaccuracies, we would not expect there to be a successful conclusion to the settlement process.

[237] Google response to November 2023 Consultation, pp.78-79; Meta response to November 2023 Consultation, pp.48-50.

3.87 Neither the substance of any oral discussions about settlement or written correspondence between the subject and Ofcom in relation to such discussions would be disclosed to the final decision maker, who is independent from the case team, so that the decision can be taken impartially, based on relevant evidence. As such, there is no need for correspondence to be treated as 'without prejudice'. However, we do not agree that additional documentary evidence that is provided during the settlement process, which is relevant to the investigation, should not be taken into account as part of the case file when reaching a provisional or confirmation decision. We also do not agree that the settlement decision maker should be independent of the case team, as Meta suggests, given that settlement is a voluntary procedure that involves the subject of the investigation accepting the case team's findings as to facts and liability. If the provider has concerns about the fairness of Ofcom's process, as set out in Section 10 of the Guidance, it is able to bring a complaint to Ofcom's Procedural Officer, who is independent from the investigation, case team, and decision makers, or to simply withdraw from settlement.

3.88 As explained at paragraph 8.6 of the Guidance, in deciding whether a case is appropriate for settlement, we take into account (among other matters) the likely procedural efficiencies and resource savings that can be achieved through settlement. We therefore disagree that a settlement discount of 30% should be given, regardless of when settlement is concluded, since the point at which settlement is agreed will generally affect the amount of resource which Ofcom must dedicate to its investigation.

Business disruption measures

3.89 Business disruption measures are orders made by a court following an application from Ofcom. They apply to third parties which are in a position to take action to disrupt the business of a provider of a service and thereby reduce the risk of harm to UK citizens and consumers. It is the decision of the court whether to grant any such application by Ofcom. This section of the Guidance sets out the different types of business disruption measures, when Ofcom might seek to apply to the courts for them, what we will take into account when deciding to do so, and the process we will follow.

Respondent comments

3.90 Five respondents gave feedback on business disruption measures, as summarised in this section. In particular, there were requests for more information about when and how we may use the measures, with a focus on access restriction orders.

3.91 Respondents asked for more information about the application of access restriction orders. For example, the Internet Service Providers' Association (ISPA) asked for information on implementation of, and compliance with, an access restriction order, timeframes, notice periods, blocking and filtering technology, and minimum standards, as well as the re-instatement process for content. It also asked when Ofcom expects to begin using business disruption powers, and whether it intends to start at high capacity or increase use of the measures over time.[238] The Internet Watch Foundation (IWF) asked whether Ofcom would offer any guidance for access facilities around the accuracy and efficiency of blocking technologies and around any appeals processes.[239]

[238] ISPA response to November 2023 Illegal Harms Consultation, pp.1-3.
[239] IWF response to November 2023 Consultation, p.41.

3.92 Three stakeholders (BT Group, ISPA and the IWF) requested further information around Ofcom's approach to identifying and engaging with access facilities during the process of applying for an access restriction order.[240] BT Group and ISPA asked that Ofcom provide the full list of facilities that it considers to meet the definition of an 'access facility' under the Act and asked for more detail on Ofcom's approach to consultation with relevant access facilities before making an application. The ISPA said that Ofcom should put in place a formal mechanism to identify the most relevant access facilities and asked whether size, technical capability, and related factors would be taken into account when considering the relevant provider to target. It said it would welcome further engagement with Ofcom around the implementation of such Orders, to ensure sufficient notice and time is given for access facilities to engage. The IWF said that Ofcom should consider whether access restriction orders need to be extended to incorporate other operators of essential internet infrastructure, such as content delivery networks and public domain name system (DNS) resolvers.

3.93 Vivastreet said it had concerns in relation to the speed and efficacy of any application for business disruption measures by Ofcom. It asked Ofcom to review the timeframe for the measures to be implemented to ensure that, where non-compliant service providers do not engage with Ofcom, the measures can be taken in short order.[241] The ISPA also noted that access restriction orders are unlikely to be effective for users of Apple devices where private relay is enabled; browsers where encryption is enabled; or a device where a virtual private network (VPN) is active.[242]

3.94 The IWF and the ISPA asked for greater clarity on how Ofcom intends to work with organisations in the UK that provide input in the blocking and filtering of content.[243] The IWF requested engagement from Ofcom on how its current blocking measures would be affected, if at all, by access restriction orders, and whether Ofcom would look to issue voluntary orders to internet service providers on its URL list.[244] BT Group and ISPA requested clarification from Ofcom about when we would consider it appropriate for providers to voluntarily block a non-compliant service.[245]

3.95 [✂].[246]

Our decisions

3.96 As set out in paragraph 9.15 of our Guidance, these measures are a significant regulatory intervention, so Ofcom is unlikely to find it appropriate to apply to the courts for business disruption measures as a matter of routine. Paragraph 9.14 of the Guidance explains that, in deciding whether it is appropriate to seek business disruption measures, we do so in line with our regulatory principles, and only where we consider it would be proportionate in the circumstances. Paragraph 9.16 of the Guidance also explains that we will take account of our priority framework in deciding whether to make an application. In particular, the level

[240] BT Group response to November 2023 Illegal Harms Consultation, pp.3-4; IWF response to November 2023 Consultation, p.41; ISPA response to November 2023 Consultation, p.3.
[241] Vivastreet response to November 2023 Illegal Harms Consultation, 2023, pp.5-6.
[242] ISPA response to November 2023 Consultation, p.3.
[243] IWF response to November 2023 Consultation, p.40; ISPA response to November 2023 Consultation, p.1.
[244] The IWF provides a list of addresses of webpages containing child sexual exploitation and abuse (CSEA) content hosted outside the UK to companies who want to block or filter them.
[245] BT Group response to November 2023 Consultation, p.4; ISPA response to November 2023 Consultation, p.2.
[246] [✂].

and degree of harm and whether there are other steps that Ofcom could take that would achieve the same ends as an application for business disruption measures.

3.97 The decisions about whether to grant an order requiring business disruption measures, and against whom, are for the court to take, not Ofcom. Therefore, while we provide guidance about the circumstances in which we may make an application for such an order, and our engagement ahead of an application with those who may be the subject to an order, the court's procedures for dealing with an application and any subsequent order it may make are a matter for the court.

3.98 Considering respondents' comments, we have made some changes to our Guidance, with a view to clarifying how we expect to engage with affected stakeholders and other entities with relevant expertise, before making an application. This may, for example, include working closely with relevant organisations to determine the most appropriate access facilities to target in any access restriction order application and to identify proportionate and effective steps for them to take to address the harm in question on a case-by-case basis.

3.99 Ofcom is currently engaging with a range of organisations, including the IWF, that have know-how related to the implementation of voluntary blocks, to understand the work they are doing and how we can support and learn from it. However, decisions around voluntary blocking are a matter for the relevant access facility. As such, we have removed the references to voluntary blocking from paragraph 9.20 of the Guidance.

Impact assessment

3.100 Generally, Ofcom will not conduct an impact assessment when publishing guidance relating to how we undertake enforcement action. The Guidance describes the procedures that we will follow when taking enforcement action against non-compliant regulated providers. These powers, and the enforceable duties, are contained in the Act, and have been subject to impact assessments through the legislative and policy making process.

3.101 Ofcom has discretion in deciding whether and how to act, such as whether to open an investigation or take informal action or apply to the court for business disruption measures. In taking these decisions we will be guided by our regulatory principles and the priority framework set out at paragraphs 3.8 to 3.10 of the Guidance, which direct enforcement action towards the most significant cases, according to:

a) the risk of harm or seriousness of the alleged conduct or contravention;
b) the strategic significance of addressing the alleged contravention; and
c) the resource implications and risks in taking enforcement action.

3.102 Providing transparency about the factors that inform the exercise of our discretion creates certainty and may encourage appropriate investment by service providers. Clarity about when enforcement action is likely incentivises compliance, deters future wrongdoing, and protects users from harm.

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

What is this chapter about?

Ofcom can recommend that service providers use proactive technology in a Code of Practice to help them to fulfil some of their duties under the Act. We can only recommend such technology to analyse user-generated content (or metadata relating to such content) that is communicated 'publicly'. Service providers looking to apply such a measure in accordance with the Codes will first need to determine which content on their service is communicated 'publicly'.

In November 2023, we consulted on high-level draft guidance to assist providers in determining whether content on their service is communicated 'publicly'. We based this draft guidance on the three statutory factors that Ofcom must consider when deciding whether content is communicated 'publicly' or 'privately' under the Act.

In this chapter, we outline the feedback that we received on our proposed guidance in the November 2023 Illegal Harms Consultation ('November 2023 Consultation') and explain the decisions that we have taken in response.

What decisions have we made?

We have considered stakeholder responses and have made the following decisions:

- We have broadly confirmed our proposed guidance with some additions to improve clarity. In particular, we have included new illustrative case studies.
- We have amended the guidance to make clear that we expect service providers to adopt a consistent approach regarding what content is communicated 'publicly' on their service, and that we consider that maintaining records could help providers to achieve this.
- We have amended the guidance to acknowledge that the fact that content is accessible to less than a substantial section of the public does not mean that it should be automatically considered as communicated 'privately'.

Why are we making these decisions? [247]

The aim of the guidance is to assist providers in determining whether content on their service is communicated 'publicly' or 'privately', so that they can apply proactive technology measures in accordance with the Codes where appropriate.

[247] The points below set out a summary of decisions relevant to the guidance. For a full account of the rationale for our decisions, see the section titled 'Our decisions'.

Many stakeholders welcomed the draft guidance. While we did receive challenges in some areas, we did not consider there to be sufficient evidence to change our approach. This has led us to largely confirm our proposed guidance.

We have made changes in response to stakeholder feedback suggesting that the draft guidance did not provide sufficient clarity. The addition of case studies, for example, is intended to help service providers better understand how Ofcom would likely approach a holistic assessment of the three statutory factors.

We also received feedback indicating that our position towards content that is accessible to less than a "substantial section of the public" was unclear. Given there can be scenarios where the other statutory factors strongly suggest content is communicated 'publicly' in this instance, we have amended the guidance to acknowledge that the fact that content is accessible to less than a "substantial section of the public" does not mean that it should be automatically considered as communicated 'privately'.

One stakeholder suggested that we should recommend in our record-keeping and review guidance that providers keep a record of how they have assessed whether content is communicated 'publicly' or 'privately' on their service. We do not consider the record-keeping and review guidance to be the appropriate channel for this. Instead, we have decided to amend our guidance on whether content is communicated 'publicly' or 'privately' to set out our expectations around taking a consistent approach to the assessment, and how keeping records can help providers to achieve this.

Introduction

4.1 Under the Act, Ofcom may include a measure recommending the use of 'proactive technology' in a Code of Practice (a proactive technology measure) as a way (or one of the ways) for providers to adhere to some of their online safety duties.[248]

4.2 Section 231 of the Act broadly defines 'proactive technology' as (i) 'content identification technology'; (ii) 'user profiling technology'; and (iii) 'behaviour identification technology', with some exceptions.[249] Proactive technology can include technologies used for automated content moderation (ACM). In Volume 2, chapter 4: 'Automated content moderation' ('ACM'), we explain our decision to recommend the use of proactive technologies by certain regulated services (specifically, the use of hash-matching for Child Sexual Abuse Material (CSAM) and URL detection for CSAM URLs). We may, in future, consider recommending other proactive technology measures across different technologies and harms.

4.3 There are several constraints on our power to recommend proactive technology measures applicable to user-to-user (U2U) services. Importantly, we may not recommend in a Code of Practice that proactive technology measures analyse user-generated content (UGC)

[248] Paragraph 13(3) of Schedule 4 of 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), 12(2), 12(3), 27(3), 29(2), 29(3), 38(1) or 39(1)).

[249] 'Content identification technology' is considered proactive technology except where this is used in response to a report from a user or other person about particular content. 'User profiling technology' meets the definition except where the technology is deployed in the circumstances referred to in section 231(5) of the Act. 'Behaviour identification technology' is exempt from this definition where this is used in response to concerns identified by another person or an automated tool about a particular user.

communicated 'privately', or metadata relating to UGC communicated 'privately.'[250] This has been reflected in each of our proactive technology measures in our first Code of Practice and would be reflected in any future proactive technology measures.[251]

4.4 Where we recommend any proactive technology measures, a provider taking such a measure will need to ensure that it applies that measure in relation to all content communicated 'publicly' by means of the service (subject to any further relevant provision). Service providers in scope of any proactive technology measures will need to determine, in the first instance, which (if any) content on their service is communicated 'publicly'.

4.5 Section 232 of the Act specifies three factors that we must consider when deciding whether content is communicated 'publicly' or 'privately.' These are:

a) The number of individuals in the United Kingdom who can access the content by means of the service;
b) 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 the provider of the service); and
c) The ease with which the content may be forwarded to or shared with:
    i) users of the service other than those who originally encounter it; or
    ii) users of another internet service.

4.6 These statutory factors should also be the starting point for providers' own assessments.

Our proposals

4.7 While we are not required to provide guidance, we proposed draft guidance in Annex 9 of the November 2023 Consultation to assist providers in determining whether content on their service is communicated 'publicly'. This is because, to apply to relevant proactive technology measures appropriately, service providers will be responsible for determining in the first instance which content on their service is communicated 'publicly'. That said, any decision on whether content is communicated 'publicly' will ultimately rest with Ofcom.[252]

4.8 We explained that our draft guidance was high-level and intended to be relevant to services of all sizes and types. As such, it was not intended to set out precisely where the boundaries between content communicated 'publicly' and 'privately' lie. We considered, however, that even high-level guidance should help to improve understanding and transparency around our approach to regulation.

4.9 We outline the primary elements of this proposed guidance in the following section.

Proposed general guidance

4.10 In summary, we proposed the following general guidance.

- The central question in the assessment is whether the *communication* of the content is public or private, rather than whether the content itself is of a 'private' nature.

[250] Paragraph 13(4) of Schedule 4 of the Act.
[251] See, in particular, measures ICU C9 and ICU C10.
[252] In its Consultation response, the Information Commissioner's Office (ICO) noted that the guidance is not an Act requirement, and that the Act does not require services to make their own assessment about whether content is communicated 'publicly' or 'privately' on their service. The ICO called for us to explain why this is our preferred approach. Source: ICO response to November 2023 Illegal Harms Consultation, p.22.

- 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 considering this. We noted that the Act does not set out that any one statutory factor should carry greater weight than another.
- We recognise that providers will need to make decisions at scale, and therefore our focus will be on the systems and processes operated in accordance with the recommended measure and their outcomes, rather than on individual pieces of content.
- Where providers identify additional factors relevant to their assessment, we expect them to record (and be able to justify) why they consider these to be relevant.
- We do not expect the fact that content has been communicated by a user that has anonymity or is using a pseudonym, or the fact that content is labelled as 'private', to be relevant to the question of whether content has been communicated 'publicly'.
- The fact that content was originally communicated 'privately' does not mean that any subsequent communications of that same content (for example, reposts by other users) should also be considered as being communicated 'privately'.

Proposed guidance on the statutory factors

4.11 In this section, we summarise our proposed guidance relating to each of the statutory factors.

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

- The more individuals in the UK are able to access the content, the more likely it is to be communicated 'publicly'. Furthermore, where content is accessible to a substantial section of the public, it should be considered as communicated 'publicly,' irrespective of the other two factors. We did not propose a specific numeric threshold for what would constitute a "substantial section of the public".
- The fact that it may be difficult for individuals to access the content, or that only a small number of users have accessed the content in practice, does not necessarily mean that content should be considered as communicated 'privately'.

(B) Access restrictions

- We provided examples of what we would and would not expect to constitute access restrictions. For example, we would expect a requirement to enter credentials (such as a password or biometrics) or to have a decryption key which is only accessible to specific individuals to constitute an access restriction, but we would not expect the same of user identity verification.
- The fact that there are access restrictions in place on a service does not necessarily, by itself, mean that content on that service is communicated 'privately'. We would still expect a service provider to consider the other statutory factors.

(C) Sharing or forwarding of content

- The focus of this factor is on: (1) any features, functionalities or settings *included* in a service which facilitate the forwarding to or sharing of content with individuals that do not already have access, and (2) the ease with which that content can be forwarded or shared by recipients (not by the person who originally uploaded or generated it).

- We provided examples of functionalities which might facilitate the forwarding or sharing of content, and examples of restrictions incorporated within functionalities which may act to limit the ease with which content may be shared or forwarded.
- The fact that it is easy to share or forward content does not necessarily, by itself, mean that content is communicated 'publicly'. Furthermore, the fact that it may be virtually impossible for providers to use technical means to prevent content from being shared (for example, by a user taking a screenshot and then sharing it) does not mean it is easy to share or forward that content.

Stakeholder responses

4.12 A number of industry stakeholders, and some civil society organisations, welcomed the draft guidance as a "helpful start" in assisting service providers to understand the distinction between content communicated 'publicly' and 'privately' as it relates to their service.[253] Snap noted that the approach strikes the appropriate balance in upholding the privacy rights of users while making progress towards safety.[254] UK Interactive Entertainment (Ukie) noted that the guidance recognises the diversity of services that may engage with it.[255]

4.13 Several stakeholders, including civil society organisations, service providers, and the Information Commissioner's Office (ICO), suggested that the draft guidance failed to provide sufficient clarity on the distinction between content communicated 'publicly' and 'privately' in some respects.[256] In particular, stakeholders sought further clarity on the first statutory factor, and what we mean by a "substantial section of the public".[257] Two civil society organisations and the ICO suggested that we should use case studies as a tool to provide greater clarity in the guidance.[258]

4.14 Several stakeholders disagreed with, or suggested changes to, elements of our general guidance and our guidance on the statutory factors. Themes raised include, but are not limited to:

---

[253] British and Irish Law, Education, and Technology Association (BILETA) response to November 2023 Illegal Harms Consultation, p.11; Google response to November 2023 Illegal Harms Consultation, p.43; Match Group response to November 2023 Illegal Harms Consultation, p.11; Meta response to November 2023 Illegal Harms Consultation, annex, p.8; NSPCC response to November 2023 Illegal Harms Consultation, p.27; Snap response to November 2023 Illegal Harms Consultation, p.13.

[254] Snap response to November 2023 Consultation, p.13.

[255] UK Interactive Entertainment Association (Ukie) response to November 2023 Illegal Harms Consultation, p.20.

[256] 5Rights Foundation response to November 2023 Illegal Harms Consultation, p.22; Canadian Centre for Child Protection (C3P) response to November 2023 Illegal Harms Consultation, p.18; Global Partners Digital response to November 2023 Illegal Harms Consultation, pp.15-16; ICO response to November 2023 Consultation, pp.22-23; International Justice Mission Centre response to November 2023 Illegal Harms Consultation, p.15; Internet Society response to November 2023 Illegal Harms Consultation, p.10; NSPCC response to November 2023 Consultation, p.27; OnlyFans response to November 2023 Illegal Harms Consultation, p.5.

[257] 5Rights Foundation response to November 2023 Consultation, p.22; Cyber Threats Research Centre, Swansea University response to November 2023 Illegal Harms Consultation, p.7; Element response to November 2023 Illegal Harms Consultation, pp.5-6; ICO response to November 2023 Consultation, p.22; Institute for Strategic Dialogue response to November 2023 Illegal Harms Consultation, pp.9-10; NSPCC response to November 2023 Consultation, p.27.

[258] 5Rights Foundation response to November 2023 Consultation, p.22; ICO response to November 2023 Consultation, p.22; NSPCC response to November 2023 Consultation, p.27.

a) calls for content to be considered as communicated 'privately' where it is difficult to access or discover[259]
b) suggestions for a presumption that content is communicated 'privately' where there are access restrictions in place[260]
c) the relevance of low maximum capacity thresholds under the guidance[261]
d) the relevance of end-to-end encryption under the statutory factors[262]
e) our approach to the ease of forwarding and sharing under the third statutory factor [263]

4.15 Some academic, civil society, and industry stakeholders also suggested that service providers (and Ofcom) should take additional factors into account beyond the three statutory factors. These included the nature of the content, the nature of the relationship between users, and the purpose of any access restrictions.[264]

4.16 We consider the comments raised by stakeholders, and set out our response to these, in more detail in the following sections.

4.17 We also set out additional stakeholder responses received, and our position on the points raised, in the Annex.

Our decisions

4.18 In the following section, we set out stakeholder views on principal themes from responses to our proposed guidance and explain how we have taken these views into account in developing our final guidance.

General guidance

Clarity

4.19 Several respondents (mostly civil society stakeholders) suggested that the guidance did not provide sufficient clarity on how providers should distinguish content communicated

[259] Apple response to November 2023 Illegal Harms Consultation, pp.11-12; techUK response to November 2023 Illegal Harms Consultation, p.24
[260] Apple response to November 2023 Consultation, p. 12; Google response to November 2023 Consultation, p.43; techUK response to November 2023 Consultation, p.24.
[261] ICO response to November 2023 Consultation, p.23.
[262] Apple response to November 2023 Consultation, pp.10-11; Big Brother Watch response to November 2023 Illegal Harms Consultation, pp.7-8; BT Group response to November 2023 Illegal Harms Consultation, p.2; BT Group supplementary response to November 2023 Illegal Harms Consultation, pp.1-3; Electronic Frontier Foundation response to November 2023 Illegal Harms Consultation, pp.1-2; Element response to November 2023 Consultation, p.5; Global Encryption Coalition response to November 2023 Illegal Harms Consultation, pp.1-2; Global Partners Digital response to November 2023 Consultation, pp.15-16; Internet Society response to November 2023 Consultation, p.11; Meta and WhatsApp responses to November 2023 Illegal Harms Consultation, annex p.7; NSPCC response to November 2023 Consultation, p.28; techUK response to November 2023 Consultation, p.23; WeProtect Global Alliance response to November 2023 Illegal Harms Consultation, p.14.
[263] Big Brother Watch response to November 2023 Consultation, p.8; International Justice Mission Centre response to November 2023 Consultation, p.15; Internet Watch Foundation (IWF) response to November 2023 Illegal Harms Consultation, p.8; Philippines Survivor Network response to November 2023 Illegal Harms Consultation, p.8.
[264] C3P response to November 2023 Consultation, p.18; Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.5-7; Institute for Strategic Dialogue response to November 2023 Consultation, p.10.

'publicly' from that communicated 'privately'.[265] The ICO, for instance, said it was important that the guidance provides sufficient direction and certainty to empower providers to make the assessment with confidence. If this is lacking, it noted that there is a risk that some providers will default to assessing content as being communicated publicly, which would undermine the effectiveness of the constraint on Ofcom's powers in practice.[266] Conversely, some respondents supported further clarity to avoid the risk that providers default to considering content as communicated 'privately', which could undermine the effectiveness of the proactive technology measures.[267]

4.20 Two civil society organisations and the ICO suggested that we should include case studies to improve the overall clarity of the guidance but had different views on what they should entail.[268] While the ICO suggested there may be particular benefit in providing clear-cut examples, the National Society for the Prevention of Cruelty to Children (NSPCC) suggested that examples might be useful for clarifying "more complex" issues.[269] In its suggestion to include case studies, the NSPCC gave the example of a large group chat of 1,001 users.[270]

4.21 We have carefully considered the calls from some stakeholders for greater clarity in the guidance. We recognise there is a risk that, in the absence of this clarity, providers may interpret the guidance in different ways – and that this could affect the effectiveness of our proactive technology measures or the constraint on Ofcom's powers.

4.22 To address this, we have included some additional case studies within our guidance which we intend to assist stakeholders and provide greater clarity. These should help service providers to understand how we would likely approach a holistic assessment of the three statutory factors.

4.23 We recognise that we could provide further detail on what we mean by a "substantial section of the public". We discuss stakeholder feedback on this, and our response, in paragraphs 4.42 to 4.49. We note that the information that the NSPCC provided in its example at paragraph 4.20 indicates that the content shared in such a group chat is likely to be communicated publicly.

4.24 We are satisfied that service providers can (and should), in the first instance, exercise a degree of discretion to determine what is content communicated 'publicly'. This is because the assessment is based on multiple factors and the outcome will therefore be specific to a service's individual circumstances. We expect providers to adopt a sensible approach to this and note that our guidance should assist them to do so. The guidance will not encourage providers to default to assessing content as being communicated 'publicly' nor 'privately'.

4.25 We can also update the guidance over time as we learn more and if we consider this would be beneficial.

---

[265] 5Rights Foundation response to November 2023 Consultation, p.22; C3P response to November 2023 Consultation, p.18; Global Partners Digital response to November 2023 Consultation, pp.15-16; ICO response to November 2023 Consultation, pp.22-23; International Justice Mission Centre response to November 2023 Consultation, p.15; Internet Society response to November 2023 Consultation, p.10; NSPCC response to November 2023 Consultation, p.27; OnlyFans response to November 2023 Consultation, p.5.
[266] ICO response to November 2023 Consultation, p.22.
[267] Institute for Strategic Dialogue response to November 2023 Consultation, p.10.
[268] 5Rights Foundation response to November 2023 Consultation, p.22; ICO response to November 2023 Consultation, p.22; NSPCC response to November 2023 Consultation, p.27.
[269] ICO response to November 2023 Consultation, p.22; NSPCC response to November 2023 Consultation, p.27.
[270] NSPCC response to November 2023 Consultation, p.27.

4.26 Furthermore, the ICO suggested that where a provider has clearly tried to follow the guidance to make this determination but is still unsure, there should be a default presumption that the content they are assessing is communicated 'privately'.[271] The ICO suggested that this would help providers to comply with their duties to avoid breaches of privacy law.[272]

4.27 While we recognise the importance of protecting users' privacy, we are not persuaded that it is necessary or appropriate for us to include such a presumption in the guidance. The statutory factors within section 232 of the Act enable both Ofcom and service providers to strike a balanced judgment on whether content is communicated 'publicly' or 'privately', recognising both the potential impact on users' privacy from the use of proactive technology as well as the potential benefits for victims and survivors and internet users from the detection of illegal content. We are concerned that the presumption suggested by the ICO could undermine the achievement of providers' online safety duties and discourage providers (and Ofcom) from achieving an appropriate balance. We are therefore not amending the guidance to include a presumption that content should be considered as communicated 'privately' where otherwise unclear.

4.28 Separately, we note that providers will need to comply with data protection requirements insofar as they are processing *any* personal data (whether or not that data is communicated 'publicly' or 'privately' for the purposes of the Act). We have amended the draft guidance to remind services of these obligations.[273]

Freedom of expression and privacy

4.29 In the November 2023 Consultation, we explained that whether content is communicated 'publicly' or 'privately' for the purposes of the Act will not necessarily align with whether that content engages users' rights to privacy under Article 8 of the European Convention on Human Rights (ECHR). This is because the assessment focuses on whether the communication of the content is public or private, rather than the content itself.

4.30 Several stakeholders raised concerns about the impact of the guidance on users' rights to freedom of expression and privacy in their responses.

4.31 Firstly, the Internet Society argued that the guidance should not suggest that the question of whether content is communicated 'publicly' does not engage Article 8 of the ECHR.[274]

4.32 We recognise that the communication of content (whether 'publicly' or 'privately') may engage users' Article 8 right to privacy.[275] However, we do not consider that the definition of content communicated 'privately' is required to align with whether that content engages users' rights to privacy under the ECHR. For example, it is possible that users might have a right to privacy under Article 8 in relation to content which is communicated 'publicly' for the purposes of the Act. Conversely, users may not have the same right in relation to

[271] ICO response to November 2023 Consultation, p.23.
[272] ICO response to November 2023 Consultation, p.23. Providers' duties about privacy are set out in section 22 of the Act.
[273] 5Rights Foundation also suggested the guidance should include a reminder of providers' duties under the UK GDPR and the Age-Appropriate Design Code. Source: 5Rights Foundation response to November 2023 Consultation, p.22.
[274] Internet Society response to November 2023 Consultation, p.10.
[275] See, in particular, footnote 5 of the guidance.

content which is communicated 'privately' for the purposes of the Act. We are therefore not making any amendments to the guidance on this point.

4.33 Secondly, some services and civil society stakeholders expressed concern about the potential effect on the right to freedom of expression if providers were to scan privately stored files using proactive technology.[276]

4.34 For the avoidance of doubt, we are unable to recommend the use of proactive technology on content communicated 'privately' and the proactive technology measures included in the Codes reflect this.[277]

4.35 We recognise, however, the potential impact that the use of proactive technology could have on users' rights to privacy and freedom of expression, as well as the benefits that this could have for victims and survivors (including children) and users.[278] We also recognise that our guidance on the concept of content communicated 'publicly' may influence the way that providers apply recommended proactive technology measures and therefore influence the impact of these measures on a range of rights.

4.36 However, any potential impacts on users' and others' rights will result from the use of proactive technology in accordance with the Code measures rather than from the guidance itself. We have also carefully considered the impacts of each of our proactive technology measures on those rights as part of our proportionality assessment of each measure. As such, we address these concerns in Volume 2, chapter 4: 'ACM', rather than in this section or in our guidance. This chapter includes a consideration of the potential interference of our ACM measures with users' rights to privacy even for content communicated 'publicly.' We also discuss the effect of our Codes and guidance more broadly in 'Introduction, our duties, and navigating the Statement', and in Volume 2, chapter 14: 'Statutory tests'.

Record-keeping

4.37 In the November 2023 Consultation, we did not propose any record-keeping guidance specific to this assessment, beyond explaining that we would expect providers to record and be able to justify any additional factors they take into consideration.

4.38 The ICO suggested that we should specifically recommend in our record-keeping and review guidance that providers should keep a record of how they have assessed whether content is communicated 'publicly' or 'privately' on their service.[279]

4.39 We do not consider it appropriate to include a specific recommendation relating to this assessment in that guidance, as it is intended to be high-level and broadly applicable across the wider record-keeping and review duties under section 23 of the Act.

4.40 We have instead amended our guidance on whether content is communicated 'publicly' or 'privately' to set out that (1) we would expect service providers to adopt a consistent approach regarding which content is communicated 'publicly' on their services and (2) that

[276] Apple response to November 2023 Consultation, pp.12-13; Big Brother Watch response to November 2023 Consultation, p.7; Google response to November 2023 Consultation, p.44.
[277] Separately, under section 121 of the Act, we have the power to issue a notice to services regulated under Part 3 of the Act and require they use accredited technology to deal with child sexual exploitation and abuse (CSEA) content on either private or public communications, which differs from our powers under Schedule 4 of the Act.
[278] Indeed, the rights of victims, including children, was emphasised by some respondents to our Consultation, such as in UK Safer Internet Centre response to November 2023 Consultation, p.2.
[279] ICO response to November 2023 Consultation, p.23.

we consider that maintaining records of this assessment could help them to achieve such consistency. In addition, keeping a written record of the assessment may support service providers to demonstrate compliance with data protection regulation.[280]

Guidance on each of the statutory factors

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

Definition of a 'substantial section of the public'

4.41 In the November 2023 Consultation, we proposed that content does not need to be accessible by all internet users to be considered as communicated 'publicly'. Instead, we proposed that content should be considered as communicated 'publicly' where it is accessible to a substantial section of the public, irrespective of the other two statutory factors.

4.42 No stakeholders disagreed with this element of our guidance. However, some stakeholders, including the ICO, called for more clarity on what we mean by a "substantial section of the public" to ensure a consistent application.[281] The Cyber Threats Research Centre at Swansea University questioned whether the assessment of what constitutes a substantial section of the public would be quantitative or qualitative, while some civil society stakeholders called for us to define it as a specific threshold or range.[282] The Institute for Strategic Dialogue suggested that, in the absence of such a threshold, Ofcom should require providers to set limits based on the nature of their services and risk assessment, which we can then assess. It expressed concern that providers could use the lack of clarity as a "loophole" to wrongly designate parts of their services as private to avoid their safety obligations.[283]

4.43 Several civil society groups expressed concern around the use of 'private' group messaging services to share illegal content.[284] Some cited large 'private' Telegram groups, which allow up to 200,000 members, being used as a loophole to circumvent legal requirements to remove illegal content including CSAM.[285] The Internet Watch Foundation (IWF) and

[280] We also note that, where a provider's assessment of whether content is communicated 'publicly' or 'privately' leads to the processing of personal data, it would need to comply with the data protection principles set out under UK GDPR. This includes the principle of accountability, which requires organisations to demonstrate compliance with data protection regulation. To demonstrate the necessity and proportionality of the data processing under this regulation, it would be reasonable for the provider in question to keep a record of its approach to whether content is communicated 'publicly', where it is relying on it to demonstrate why it considers the processing of personal data to be necessary. For more information, see ICO, Content moderation and data protection. [accessed 25 November 2024].

[281] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.6-7; ICO response to November 2023 Consultation, pp.22-23; Institute for Strategic Dialogue response to November 2023 Consultation, pp.9-10; NSPCC response to November 2023 Consultation, p.27.

[282] 5Rights Foundation response to November 2023 Consultation, p.22; Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.6-7; ICO response to November 2023 Consultation, pp.22-23; NSPCC response to November 2023 Consultation, p.27.

[283] Institute for Strategic Dialogue response to November 2023 Consultation, p.10.

[284] C3P response to November 2023 Consultation, p.18; Institute for Strategic Dialogue response to November 2023 Consultation, p.10; NSPCC response to November 2023 Consultation, pp.27-28; WeProtect Global Alliance response to November 2023 Consultation, p.14.

[285] C3P response to November 2023 Consultation, p.18; Institute for Strategic Dialogue response to November 2023 Consultation, p.10.

Element also queried how many users must be part of a group within a so-called 'private' service before content is communicated 'publicly'.[286]

4.44 We have carefully considered the calls from some stakeholders for greater clarity about how to define large group chats and what constitutes a substantial section of the public.

4.45 As discussed in paragraph 4.21, we recognise that there is a risk that service providers adopt different approaches to what is meant by a "substantial section of the public", which could affect the effectiveness of our proactive technology measures or the constraint on Ofcom's powers.

4.46 The case studies discussed in paragraph 4.22 will provide additional clarity to assist service providers in taking each of the three statutory factors into account. We recognise that we could provide further clarity on "substantial section of the public" by including quantitative figures or ranges in the case studies or within the guidance more generally. However, we are not persuaded that additional guidance of this nature is required at this stage.

4.47 We reiterate our position expressed in paragraph 4.24 that service providers can (and should), in the first instance, exercise a degree of discretion to determine what in their view is content communicated 'publicly', and that we expect providers to adopt a sensible and reasonable approach to this. We will keep the guidance under review and may update it over time where appropriate.

4.48 On the suggestion to require providers to set limits based on the nature of their services and risk assessment, we do not consider that a service's risk assessment, or the nature of the service, are relevant to the question of whether content is communicated 'publicly', or 'privately.' We do not expect that either factor would influence what is a "substantial section of the public", and so have not amended the guidance on this point.

4.49 Separately, the Cyber Threats Research Centre at Swansea University suggested that the guidance should explicitly state that the fact that content is accessible to a section of the public that is less than substantial does not mean that the content is communicated 'privately,' for consistency with the 'Encouragement of Terrorism' offence (Terrorism Act 2006, s.1).[287] To avoid confusion, we have amended the guidance to acknowledge that the fact that content is accessible to less than a "substantial section of the public" does not mean that it should be automatically considered as communicated 'privately'. It is possible in this scenario that the other two statutory factors, taken together, could strongly indicate that content is communicated 'publicly'.

Discoverability

4.50 In the November 2023 Consultation, we explained that the fact that it may be difficult for individuals to discover the content does not mean that content should be considered as communicated 'privately'.

4.51 Two industry stakeholders argued that, even if there are no formal access restrictions in place and content is 'technically' accessible to a substantial section of the public, it should be considered as communicated 'privately' if it is difficult to access or discover.[288] Apple

[286] Element response to November 2023 Consultation, pp.5-6; IWF response to November 2023 Consultation, p.8.
[287] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, p.7.
[288] Apple response to November 2023 Consultation, pp.11-12; techUK response to November 2023 Consultation, p.24.

expressed concern we had taken an "unduly narrow approach" to the meaning of a person being 'able' to access content, and instead argued that should be interpreted as meaning that the person has "all the necessary means to access" that content, including all the necessary information to locate it.[289] techUK gave the example of content which can theoretically be accessed by a wide group, but in practice is only accessible where those users have been given a URL that is not otherwise discoverable.[290]

4.52 We maintain that where content is accessible by many people, it should be considered as communicated 'publicly' even where it is difficult to discover. We would expect that, had Parliament intended the first statutory factor to focus on how many users are able to access the content with 'ease', it would have made this explicitly clear in section 232 of the Act as has been the case for the third statutory factor ('ease of sharing or forwarding content').

4.53 In the example of a complex URL that is not discoverable (see paragraph 4.51), there would be no formal access restrictions in place. This would mean that, in principle, the communication could be accessed by all internet users. We consider that it would be inconsistent with the statutory factors and could risk undermining the online safety objectives if we were to treat such content as communicated 'privately'.[291]

Access restrictions (B)

Presumption that content is communicated 'privately' where there are access restrictions in place

4.54 In the November 2023 Consultation, we proposed that the fact that there are access restrictions on a service does not necessarily mean, by itself, that content on that service is communicated 'privately'.

4.55 Some industry stakeholders have suggested that where clear access restrictions are in place, content should always be considered as communicated 'privately,' irrespective of the number of users who are able to access it.[292] techUK and Apple suggested that, at the very least, providers should assume by default that content is communicated 'privately' where there are access restrictions, unless there are clear factors suggesting otherwise.[293] Stakeholders argued that this would better align with users' expectations of privacy and avoid subjecting content communicated on file-sharing or storage services with restricted access controls to proactive technology measures.[294]

4.56 In response to industry stakeholders' suggestions to include a presumption that content is private where there are access restrictions in place, we are maintaining our position that the fact that access restrictions are in place does not necessarily mean, by itself, that content is communicated 'privately.' The suggested presumption would disregard two of the statutory factors that we are required to consider under section 232 of the Act. We expect providers to make a holistic assessment, taking account of each of the factors and

[289] Apple response to November 2023 Consultation, p.11.
[290] techUK response to November 2023 Consultation, p.24
[291] The online safety objectives are set out in Schedule 4 of the Act.
[292] Google response to November 2023 Consultation, p.43; techUK response to November 2023 Consultation, p.24.
[293] Apple response to November 2023 Consultation, p.12; techUK response to November 2023 Consultation, p.24.
[294] Apple response to November 2023 Consultation, p.12; techUK response to November 2023 Consultation, p.24.

consider how many individuals in the UK can access the content, and the ease with which it can be forwarded or shared, even where there are access restrictions in place. This is consistent with the wording of section 232 of the Act, which does not ascribe greater weight to any one of the three statutory factors over the other.

End-to-end encryption

4.57 One of the examples of access restrictions that we proposed in the draft guidance was a requirement for users to have access to a decryption key to access the content (where that key is only available to specific individuals). However, as noted in paragraph 4.56, we have made it clear that the presence of an access restriction on a service, by itself, does not necessarily mean that content on that service is communicated 'privately'.

4.58 Two civil society organisations recommended that the guidance should be amended to explicitly reference encryption as a factor that providers should take into account when determining whether content should be considered as having been communicated privately.[295] Element sought clarity on how the statutory factors would apply where end-to-end encryption is present by default.[296]

4.59 Some stakeholders went further, suggesting that the guidance should make clear that end-to-end encrypted content should always be considered as communicated 'privately,' and should therefore not be subject to any ACM measures.[297] Big Brother Watch and the Internet Society highlighted that the purpose of end-to-end encryption is to protect the privacy of users' communications, and, alongside Apple, expressed concern that services that use E2EE are not able to analyse user-generated content in the way required by the ACM measures and therefore the proposed measures would not be technically feasible on E2EE services.[298] The Electronic Frontier Foundation cited a recent ECHR judgement that noted that the weakening of end-to-end encryption can lead to "general and indiscriminate surveillance of personal communications."[299]

4.60 Conversely, BT Group and some civil society organisations argued that end-to-end encrypted content should not necessarily be considered as content communicated 'privately'.[300] Both BT Group and the NSPCC expressed concern at our proposal to exclude end-to-end encrypted services from the first iteration of proactive technology measures.[301] We address this concern in Volume 2, chapter 4: 'ACM'.

4.61 We recognise that there has been some confusion among stakeholders, some of whom have understood our position to be that all content communicated on end-to-end encrypted parts of a service should be considered as communicated 'privately'. In support

---

[295] Global Encryption Coalition response to November 2023 Illegal Harms Consultation, p.2; Global Partners Digital response to November 2023 Consultation, p.16.
[296] Element response to November 2023 Consultation, p.5.
[297] Apple response to November 2023 Consultation, pp.10-11; Big Brother Watch response to November 2023 Consultation, p.7; Internet Society response to November 2023 Consultation, p.11; techUK response to November 2023 Consultation, p.23.
[298] Apple response to November 2023 Consultation, pp.10-11; Big Brother Watch response to November 2023 Consultation, p.7; Internet Society response to November 2023 Consultation, p.11.
[299] Electronic Frontier Foundation response to November 2023 Consultation, p.2.
[300] BT Group response to November 2023 Consultation, pp.2-3; BT Group supplementary response to November 2023 Consultation, p.2; IWF response to November 2023 Consultation, p.8; NSPCC response to November 2023 Consultation, p.28.
[301] BT Group response to November 2023 Consultation, p.3; BT Group supplementary response to November 2023 Consultation, p.2; NSPCC response to November 2023 Consultation, p.28.

of this view, some stakeholders referenced our provisional view that our proposed CSAM hash matching and CSAM URL detection measures would not be technically feasible for end-to-end encrypted content.

4.62 For the avoidance of doubt, we disagree with the interpretation that content that is communicated on a service that is end-to-end encrypted should always be considered as communicated 'privately'. As set out in the decryption key example in the draft guidance (paragraph A9.28), end-to-end encryption is an access restriction and is therefore relevant to the consideration of the second statutory factor.[302] We acknowledge that where content is communicated that is end-to-end encrypted, the use of end-to-end encryption is indicative that the content in question is communicated 'privately'. We would however still expect the service provider to consider information reasonably available to it about how many individuals in the UK are able to access the content, and the ease with which it can be forwarded or shared. We are therefore not amending the guidance to state that content communicated on a service that is end-to-end encrypted is always communicated 'privately'.

4.63 Furthermore, the question of whether content should be considered as communicated 'publicly' or 'privately' is distinct from the question of whether it is 'technically feasible' for a service provider to implement a particular measure in relation to that content. Nothing in our Codes recommends a provider should do anything that is not technically feasible. This is the case even if that content is communicated 'publicly'.[303]

Low maximum capacity thresholds

4.64 In our November 2023 Consultation, we proposed that, for the purposes of the first statutory factor, content should be considered as accessible to all UK internet users if there are no access restrictions in place. The ICO sought clarity as to whether this would also be the case where a service is configured to have low maximum capacity thresholds.[304]

4.65 We recognise that the guidance was not clear on this point and may have been read as suggesting that low maximum capacity thresholds (which we understand as referring to restrictions on how many users may concurrently access content) are not relevant to the question of whether content is communicated 'publicly' or 'privately'.[305]

4.66 Our view remains that such thresholds do not constitute access restrictions (in the sense that they do not restrict who may access the content, but instead how many people may access the content at a *particular point in time*). However, we have amended the guidance to explain that service providers may wish to consider such thresholds when determining the number of UK users able to access the content under the first statutory factor (even if those thresholds are not an access restriction under the second statutory factor).

---

[302] In its Consultation response, Element queried whether the fact that communicating content via encrypted services requires an account would mean it is a blanket access restriction. For the avoidance of doubt, E2EE is an access restriction, regardless of whether or not it requires an account. Source: Element response to November 2023 Consultation, p.6.

[303] We also note that where an action is technically not feasible, but for only part of a service, the provider would need to take the action for the parts of the service for which it is technically feasible.

[304] ICO response to November 2023 Consultation, p.23.

[305] See, in particular, paragraph A9.31 of our draft guidance. We noted in the final bullet of that paragraph that we did not consider the following to be an access restriction: "[T]he fact that the technical design of the service means that it has only limited capacity to accommodate concurrent users".

Sharing or forwarding of content (C)

4.67 In our November 2023 Consultation, we acknowledged that it may be possible for content to be shared or forwarded from any internet service, and that it may be virtually impossible for services to use technical means to prevent online content from being shared in this way. We set out that we do not expect this to indicate that content can be forwarded or shared with ease for the purpose of this third statutory factor.

4.68 Several civil society organisations noted that content that might be assumed to be private or not easily shareable could, in fact, be communicated 'publicly' if it is screenshotted or recorded via software or a secondary device and then shared (either online or in person).[306] The IWF highlighted the relevance of this for self-generated CSAM in particular, and argued that the draft guidance does not fully explore this issue. It provided the example of such material being shared between two teenagers in a romantic relationship, but then shared more widely when that relationship breaks down.[307]

4.69 As noted in paragraph 4.67, we do not consider the fact that a user can covertly take a screenshot or record the content in some way to be relevant to the ease of sharing or forwarding under the second statutory factor. If the ability for content to be screenshotted or recorded covertly were relevant, this might result in an overly wide interpretation of what is communicated 'publicly'. We are therefore maintaining our position, as set out in the November 2023 Consultation, that the focus of this factor should be on any features, functionalities, or settings included in a service which facilitate the forwarding to or sharing of content with individuals that do not already have access to that content. This includes, for example, a 'reposting' or 'tagging' functionality.

4.70 Separately, we recognise the concern that just because content might first be communicated 'privately,' this does not necessarily mean that all subsequent communications of that content should also be considered 'private'. In this instance, we would expect the latter to be a new communication of content, and so the provider should consider the communication of this content on its own merits. We are satisfied that the guidance already adequately addresses this concern although we have added a case study to the guidance on this point to provide greater clarity to providers.

4.71 In addition, Big Brother Watch expressed concern that the draft guidance suggests content might be communicated 'publicly' due to the "possibility, rather than actuality" of content being shared.[308]

4.72 Section 232 of the Act is clear that the third statutory factor relates to the ease with which content "may" be forwarded or shared. Furthermore, we consider that requiring evidence that content has in fact been shared or forwarded with ease would set an unduly high threshold, which could undermine the online safety objectives.

4.73 We are therefore retaining our proposed guidance that this factor requires a qualitative judgement to be made about the ease with which content *may* be subsequently shared or forwarded, rather than whether it has been forwarded or shared. We note, however, that while evidence of content being shared or forwarded with ease is not *required* to

[306] International Justice Mission Centre response to November 2023 Consultation, p.15; IWF response to November 2023 Consultation, p.8; Philippines Survivor Network response to November 2023 Consultation, p.8.
[307] IWF response to November 2023 Consultation, p.8.
[308] Big Brother Watch response to November 2023 Consultation, p.8.

demonstrate the ease with which that content "may" be forwarded or shared, evidence that content has in fact been shared with ease is likely to be highly relevant when considering this third statutory factor.

Suggestions for additional factors

4.74 In our November 2023 Consultation, we recognised that providers may identify one or more additional factors which they consider relevant to assessing whether content has been communicated 'publicly' on their service. We explained that, in this case, we would expect providers to record and be able to justify why they consider these to be appropriate. We also provided some examples of factors that we would not expect to be relevant to this assessment, including whether a user has anonymity or uses a pseudonym, or the fact that content is labelled as 'private'.

4.75 Some academic, civil society, and industry stakeholders suggested additional factors that providers (and Ofcom) should consider in making the assessment.

a) **The nature or purpose of the content**: The Cyber Threats Research Centre at Swansea University suggested that the nature of content may inform the assessment of whether content is communicated 'publicly' in some scenarios. It gave the example of an official magazine of a proscribed terrorist organisation that might initially be shared between a smaller group for onward distribution to a larger one. It suggested that, in this example, the intention to widely disseminate the content should inform the assessment of the initial communication.[309]
b) **The nature of the group, or the relationships between users of a channel or community:**[310] The Canadian Centre for Child Protection (C3P) suggested that there should be consideration of the nature of groups formed to share CSAM in particular.[311] The Cyber Threats Research Centre also noted that anonymity can be indicative of users' intentions to limit access to a certain section of the public in certain scenarios, for instance, those who sympathise with proscribed terrorist groups. It suggests that anonymity can therefore indicate that content should be considered as communicated 'publicly'.[312]
c) **The purpose or practical operation of the access restrictions:**[313] The Cyber Threats Research Centre gave an example of private channels used by terrorist groups where the use of access restrictions can perversely work to increase later dissemination and make the content more publicly available.[314] C3P also noted how the purpose of access restrictions can be to evade detection by law enforcement.[315]
d) **The expectations of users to privacy when communicating:** One service provider noted that the guidance does not take account of the "reasonable expectations" of users to privacy by adopting too narrow a definition of 'content communicated privately'.[316]

---

[309] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.5-6.
[310] C3P response to November 2023 Consultation, p.18; Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.5-6; Institute for Strategic Dialogue response to November 2023 Consultation, pp.9-10.
[311] C3P response to November 2023 Consultation, p.18.
[312] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, p.5.
[313] C3P response to November 2023 Consultation, p.18; Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.5-8.
[314] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, pp.7-8.
[315] C3P response to November 2023 Consultation, p.18.
[316] Apple response to November 2023 Consultation, p.12.

techUK argued that content should not be subject to proactive technology requirements (in that it is communicated 'privately') unless the user explicitly indicates that it expects the content to be shared publicly.[317]

e) **The extent to which a service enables access to content by means of another service:** The Cyber Threats Research Centre suggested that the providers of "aggregator" services (which it defines as services that provide lists of URLs from which propaganda materials can be downloaded), should have to consider the extent to which they enable access to content by means of another service.[318]

4.76 As explained in the November 2023 Consultation, we recognise that providers will need to make decisions about whether content is communicated 'publicly' at scale. We therefore do not expect providers to make judgements at the level of individual pieces of content present on their service. As set out in the draft guidance, our focus will be on the systems and processes operated for this purpose and their outcome.

4.77 As such, we would not expect service providers to consider the nature or purpose of the content, the nature of the group in which it is shared, nor the purpose of any access restrictions that are applied to it. Making the assessment at such a granular level would likely require providers to use proactive technology to analyse content to determine whether content is communicated 'publicly', which would undermine the restriction on our power to recommend the use of proactive technology.[319]

4.78 The examples of anonymity that the Cyber Threats Research Centre provided in its response are indicative of how anonymity can be a relevant factor in assessing the risk of illegal content being present on a service. However, it is not clear from the evidence provided that having anonymity is directly relevant to whether content is communicated 'publicly' or 'privately'. We are therefore retaining our guidance on anonymity and pseudonymity as proposed.

4.79 In relation to the practical operation of access restrictions, we recognised in the November 2023 Consultation that there may be limits to the provider's knowledge about the number of users that are in fact able to access content where access restrictions are in place. For example, a user may choose to share the password for their account with other users without the provider's knowledge. We therefore expect providers to make their assessment of whether content has been communicated 'publicly' or 'privately' based on the information reasonably available to them, which may not necessarily align with the practical operation of any access restrictions.

4.80 We are not persuaded that specific additional guidance is required around 'aggregator' services. Providers of services of this nature that are in scope of the Act will need to consider whether they are in scope of any proactive technology measures following their risk assessment. If this is the case, they should undertake an assessment based on the three statutory factors set in section 232 of the Act, as for any other type of regulated service. We understand that by facilitating access to other content by means of another service, the Cyber Threats Research Centre is referring to the URLs that 'aggregator' services provide

[317] techUK response to November 2023 Consultation, p.24.
[318] Cyber Threats Research Centre, Swansea University response to November 2023 Consultation, p.7.
[319] Schedule 4, paragraph 13 of the Act.

which link to third-party services. Such URLs would be considered as content under the Act, and therefore would be in scope of this assessment.[320]

[320] See, in particular, the section titled 'Use of URL links' in Ofcom's Illegal Content Judgment Guidance.

A1. Annex to Volume 3

Introduction

A1.1 It is true to say that the Act applies to content where content amounts to a relevant offence within the UK illegal in the UK and visible to UK users. However, this interpretative rule in the Act applies only to what happens in relation to the content. It does not affect, for example, any offline circumstances required for the offence to be committed.

A1.2 In this annex, we outline our reasons for our decisions on the proposals which we set out in our consultation document regarding the Illegal Contents Judgements Guidance (ICJG) which were not subsequently challenged by stakeholders or changed by Ofcom.

Cross-cutting decisions

Mens rea or the mental element of an offence

A1.3 The 'mental element' of the offence refers to the state of mind of the person who is potentially committing an offence. In legal terminology this is known as 'mens rea.' It must be satisfied in order for reasonable grounds to infer to exist. Neither Ofcom nor in-scope service providers can put aside the state of mind or 'mental element' requirement as this is a part of the 'reasonable grounds to infer' threshold established by the Act.

Inferring conduct, behaviour and state of mind when content has been posted by a bot

A1.4 Section 192 of the Act states that where content has been posted by a bot, inferences about the conduct and the presence of the mental element, and any defences, should be made by considering:

a) the actual person controlling the bot or tool, where this is known to the service; or
b) the person who may be assumed to be controlling the bot, where the actual identity of the person is not known.

A1.5 We have concluded that this inference will normally be fairly straightforward to apply, since the analysis will not be very different whether the content is posted by a human directly or by a human controlling a bot. However, it may make a substantive difference to judgements about the foreign interference offence. As such, we have decided to provide general principles in relation to bots in our offence-agnostic introductory sections, and specific guidance on making inferences in relation to bots for foreign interference offences only.

Inferring presence of satisfaction of the mental element of 'knowledge'

A1.6 Several priority offences, including offences to do with child abuse imagery or possession of extreme pornography, include a state of mind requirement (or 'mental element') of 'knowledge'. For an offence to have occurred a defendant must know that what they have uploaded or shared etc was the image in question.

A1.7 We consider it is reasonable to infer that users are aware of the nature of the content they upload as we do not consider it plausible that most users are unaware of the nature of most content they upload. We are aware that there is research to suggest that a significant

and perhaps a very significant minority of users do not look at content they forward. However, we consider that most do, and that it is therefore reasonable to infer that users who forward and onward share content *are* aware of what it is. We have adopted an approach to inference of the mental element of knowledge in line with this reasoning, adapting it on an offence-by-offence basis.

Inferring presence of satisfaction of 'possession'

A1.8 Sometimes the conduct part of an offence occurs when content is 'possessed'. 'Possession' is defined as being met when the images are in the custody or control of the suspect i.e. so that they are capable of accessing, or in a position to retrieve the image(s); and the suspect must have known that they possessed an image or group of images on the relevant device. In addition, the definition of illegal content includes that 'content consisting of certain… images… amounts to a relevant offence if… the possession… of the content constitutes a relevant offence'. We consider that service providers may therefore reasonably infer that if the content appears, 'possession' is met.

Terrorism

Miscellaneous specific terrorism offences

Publishing information about members of the UK armed forces etc.

A1.9 The offence of publishing information about members of the UK's armed forces, UK intelligence services or a constable (a UK police officer) is one which may not be obvious to service providers. It is rarely prosecuted, so there is not much information available on how to interpret it. Many soldiers and police officers have social media accounts. We have therefore decided to say in our guidance that, for example, information on the specific location or activity of military units during a specific current or future time period may be information of a type likely to be useful to a person committing or preparing an act of terrorism.

A1.10 We note that there is a defence of 'reasonable excuse'. We believe that such a defence may be reasonably inferred where the true purpose of the publication is academic or journalistic. For example, reasonable excuse may exist where a journalist or academic shares information on military exercises or movements in a way that presents them as matters of historical or journalistic record and which could not be reasonably said to risk the safety of the personnel involved.

Terrorist threats and directing a terrorist organisation

A1.11 Although the final ICJG covers the offences of making terrorist threats and directing a terrorist organisation, we have decided do so only briefly because we provisionally consider that in practice content which amounts to these offences will also amount to other less specific priority offences. This is because terrorist threats can be considered along with other kinds of threats (we consider other kinds of threats in the section on 'Threats, abuse and harassment (including hate)'). The offence of directing a terrorist organisation is likely to be very difficult for service providers to identify. If the content is sufficiently clear to make an illegal content judgement, it would likely also amount to the offence of preparation of terrorist acts.

Threats, abuse and harassment (including hate)

Broad approach to the chapter

A1.12 The priority offences which relate to threats, abuse and harassment overlap with one another to a very significant degree. It is therefore likely to be repetitive and inefficient for service providers to consider each offence in turn. In the ICJG we therefore approach this chapter in a thematic manner, grouping offences by type, rather than going through offence by offence as we have with the majority of other chapters in the ICJG. This will allow providers to work through several complicated and interlinked offences in a manageable and efficient way. Therefore, service providers are to consider all the offences to do with threats first, then those which involve insults/abuse, before moving on to the offences which are more specific.

A1.13 Our chapter on threats, abuse and harassment (including hate) sets out our approach to the following priority offences relating to race, religion, and sexual orientation:

a) Offences relating to the stirring up of hatred on the basis of race, religion and sexual orientation (Public Order Act 1986[321]); and
b) Other priority offences which concern:
    i) racially-aggravated harassment[322]; and
    ii) the commission of offences under the Public Order Act 1986 and the Protection from Harassment Act 1987[323] which are racially or religiously aggravated.[324]

Threatening and abusive behaviour

A1.14 There are a number of different priority offences which may be committed by threats, and a slightly smaller number by abuse. In the ICJG, we consider the broadest, and therefore most important offence of the threatening and abusive behaviour group to be section 38 of the Criminal Justice and Licensing (Scotland) Act 2010 (asp.10) (the 'section 38 offence'). This offence is committed if a person behaves in a threatening or abusive manner, and the behaviour would be likely to cause a reasonable person to suffer fear or alarm. The state of mind requirement is that the person intends by the behaviour to cause fear or alarm or is reckless as to whether the behaviour would cause fear or alarm. There is a defence if the behaviour was, in the circumstances, reasonable. We note that this offence is broader due to the 'recklessness' requirement which is the same as in Scottish law generally, and which indicates that a person 'failed to think about or were indifferent' as to whether fear or alarm would result from their behaviour. We also note that the offence is broader because

[321] Specifically: section 18 (use of words or behaviour or display of written material); section 19 (publishing or distributing written material); section 21 (distributing, showing or playing a recording); section 29B (use of words or behaviour or display of written material); section 29C (publishing or distributing written material); and section 29E (distributing, showing or playing a recording).
[322] Section 50A(1)(a) and (b) Criminal Law (Consolidation) (Scotland) Act 1995. This has subsequently been repealed.
[323] Sections 31 and 32 of the Crime and Disorder Act 1998.
[324] We are aware that for sentencing purposes, any offence is to be treated as aggravated if it demonstrated or was motivated by racial hostility, religious hostility, hostility related to disability, hostility on the basis of sexual orientation, or hostility related to transgender identity, as set out in section 66 of the Sentencing Act 2020. However, the presence or absence of an aggravating factor for sentencing purposes is not material to the identification of illegal content under the Act.

it does not need to be a threat of 'immediate' violence in the case of the section 38 offence. The offence also overlaps greatly with most of the other 'threat' and 'abuse' offences but is easier to show than most of them. Service providers should therefore consider it first, but not *alone*. The reasoning for the threats offences is as follows:

a) The two important non-overlaps with section 38 are the offences in section 5 of the Public Order Act 1986 (threatening and abusive conduct) and in sections 18, 19 and 21 of the same Act (stirring up racial hatred). Where section 5 talks about threatening or abusive conduct which is likely to cause alarm, it overlaps with the section 38 offence. However, it can also be committed when the threatening or abusive conduct is likely to cause no alarm, but only harassment or distress. Harassment in particular is a fairly low threshold. However, content likely to cause harassment or distress will only be illegal content if there are reasonable grounds to infer that the person posting it was at least aware that what they were doing may be threatening or abusive, and that a person likely to be caused harassment or distress was nearby. This tends to make the offence less likely to be identifiable in practice.

b) Threatening and abusive conduct likely to stir up racial hatred is next. In practice much content which is likely to stir up racial hatred is also likely to amount to the section 38 offence, which is easier to show and should therefore be considered first. It is also possible that as set out above it may amount to the section 5 offence. However, in theory it is possible that content could exist which, even though it was likely to stir up hatred, was neither likely to cause a reasonable person to suffer fear or alarm nor was used within sight or hearing of a person likely to suffer harassment or distress. In that case, providers would need to go on to consider whether it was likely to stir up racial hatred.

c) Similar reasoning applies to conduct likely to stir up religious hatred or hatred on grounds of sexual orientation, but for these offences there must be intent to stir up hatred.

d) Finally, to the extent that the section 4 Public Order Act offence relates to fear of violence, it overlaps with the section 38 offence, and because it only relates to immediate violence it is unlikely to take place online in any event. But very rarely, content online may provoke immediate violence – for example in the context of ongoing serious public disorder. In that case, providers would need to consider the section 4 Public Order Act offence.

Epilepsy trolling

A1.15 In the draft guidance we included guidance on one non-relevant priority offence in the chapter on threats, abuse and harassment (including hate): the newly created epilepsy trolling offence. We proposed to provide guidance on this offence because the type of conduct concerned is likely also to potentially amount to harassment, but epilepsy trolling may be easier to show since there is no need to show that there has been a course of conduct. We have decided to go ahead with the inclusion of the epilepsy trolling offence in the ICJG, although as noted above it will now sit within a separate chapter on non-priority offences.

Child sexual exploitation and abuse (CSEA) - Grooming and exploitation of children

A1.16 The child sexual exploitation and abuse offences that sit within the chapter that we have called 'Grooming and Exploitation of Children' are more complex to identify in practice than the offences covered in the chapter on offences relating to child sexual abuse material (CSAM).

Meeting a child offences

A1.17 The priority offences that relate to grooming and exploitation of children include offences related to meeting a child following sexual grooming or preliminary contact. Meeting in relation to these offences means a physical, face-to-face encounter in the real world rather than online (unlike the terrorism offences). For this reason, we do not deal with the 'meeting' offences in our guidance. However, the preceding communications leading up to the offence may amount to illegal content by virtue of one or more of the other priority offences[325], and any online 'meeting' which is unlawful is likely to amount to one or more other priority offences too.[326]

Sexual exploitation of a child

A1.18 The offences relating to sexual exploitation of children are designed to penalise those involved in child sexual exploitation at many levels. For example, the offence of controlling a child aged 17 or younger in relation to sexual exploitation, would capture the activities of a person at a higher level of a criminal gang involved in the exploitation, as well as the gang member directly controlling a child day-to-day.

A1.19 However, the more remote from the child victim the individual is, the greater the evidential difficulties of proving that the content amounts to the offence are likely to be. We consider that the child exploitation offences that service providers are most likely to encounter online will be when, in the content being considered, a child is being incited or coerced into providing indecent images of themselves online.

A1.20 We note that the child exploitation offences have a fairly high state of mind requirements. First, where the child is over 13, the service provider must have reasonable grounds to infer that the potential perpetrator did not reasonably believe that the potential victim was 18 or over. We recognise that a provider is not likely to have a direct statement from the

[325] For example, sexual communication with a child (section 15A of the Sexual Offences Act 2003; Article 22A of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2)); or communicating indecently with
a child (sections 24 and 34 of the Sexual Offences (Scotland) Act 2009).

[326] For example, causing or inciting a child to engage in sexual activity (sections 8 and 10 Sexual Offences Act 2003; Articles 15 and 17 of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2)), causing a child to watch a sexual act (section 12 of the Sexual Offences Act 2003); Article 19 of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2), arranging or facilitating commission of a child sex offence (section 14 of the Sexual Offences Act 2003; Article 21 of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2)); sexual communication with a child (section 15A of the Sexual Offences Act 2003; Article 22A of the Sexual Offences (Northern Ireland) Order 2008 (S.I. 2008/1769 (N.I. 2)); causing a child to participate in a sexual activity (sections 21 and 31 of the Sexual Offences (Scotland) Act 2009); causing a child to look at a sexual image (sections 23 and 33 of the Sexual Offences (Scotland) Act 2009); communicating indecently with a child (sections 24 and 34 of the Sexual Offences (Scotland) Act 2009).

potential perpetrator of their beliefs, reasonable or otherwise. More importantly, it would be a very great interference with users' rights if service providers were to go looking in their account activity for evidence of potential perpetrators' beliefs, and perhaps the activity of other users to see whether they had said or done anything to make a belief reasonable.

A1.21 However, our view is that if the service provider itself is in a position to infer that the potential victim is under 18, it is sufficiently obvious that a potential perpetrator's belief is unlikely to be reasonable.

A1.22 Secondly, the possible perpetrator must have intent – for example, for the offence of obtaining the sexual services of a child, the potential perpetrator must intend to obtain sexual services. Again, we recognise that in these types of instances, the potential perpetrator is unlikely to have stated their intent explicitly. However, our view is that where content is identifiable by a service as meeting the 'conduct' part of the offence (for example, if the content comprises a direction to the child to provide sexual services, coupled with an offer of payment), it is reasonable to infer that the state of mind requirements are also met. It is difficult to conceive of any reason why a person would send such a request, absent that intent.

Fraud and other financial offences

False claims to be authorised or exempt

A1.23 Out of all the fraud and financial services offences, services should first consider whether the firm offering those services is claiming to be authorised. That is because it should be relatively straightforward for providers to identify content containing a false claim to be authorised or exempt. Determining whether a claim to be authorised is true is a fairly straightforward matter of checking the content, including address and other contact details, against a register the FCA publishes on its website (the Financial Services Register ('FS Register')). We consider that this is a check providers can be expected to make where alerted to a possible false claim to be authorised. We believe a provider will have reasonable grounds to infer that a claim to be authorised is false and the content is illegal content if the firm is not included as an authorised firm on the FS Register or the details referred to in the online content do not match the details of the authorised firm on the FS Register. Similarly, the FCA gives firms a unique Firm Reference Number (FRN) when the firm becomes authorised. Using an FRN which does not appear on the FS Register, or providing different contact details than those included on the FS Register would in our view provide reasonable grounds to infer that the content contains a false claim to be authorised.

A1.24 This is, however, only one of the priority financial services and markets offences. The other offences are some of the most technically difficult offences in the Act to interpret. We have therefore structured the chapter on these offences in a way which is intended to enable services to capture the relevant content most easily. For that reason, we do not deal with the more complex financial services and markets acts offences until later in the chapter, and instead steer providers to next consider fraud by false representation.

Approach to articles for use in frauds

A1.25 It is an offence to make, adapt, supply or offer to supply any article, knowing that it is designed or adapted for use in the course of or in connection with frauds. It is also an offence to make, adapt, supply or offer to supply any article, intending that it be used to commit, or assist in the commission of, fraud. An 'article' includes data or software. We are aware that both search and U2U services are used to offer to supply, and sometimes to supply, data and/or software for use in frauds – for example, lists of stolen passwords.

A1.26 While the state of mind requirement for this offence is fairly high (intent), our view is that in practice, it is difficult to conceive of any reason why a person would be disseminating or offering to disseminate certain information online, other than for use in a fraud.

Approach to buying and selling offences

A1.27 Schedule 7 of the Act includes priority offences relating to the marketing, buying and selling or supply of drugs/psychoactive substances and of weapons. We refer to these in the ICJG and here as the 'buying and selling offences.' They raise particular interpretive challenges in relation to jurisdiction.

A1.28 The general purpose of the Act is to make the use of regulated internet services safer for individuals in the United Kingdom. The safety duty extends only to the design, operation and use of the service in the United Kingdom, and in the case of a duty that is expressed to apply in relation to users of a service, the design, operation and use of the service as it affects United Kingdom users of the service.

A1.29 However, the definition of illegal content is not limited to conduct that takes place in the UK or that affects UK users. The Act states that "[f]or the purposes of determining whether content amounts to an offence, no account is to be taken of whether or not anything done in relation to the content takes place in any part of the United Kingdom." The Explanatory Note to the Act explains that the effect of this is that "content does not need to be generated, uploaded or accessed (or have anything else done in relation to it) in any part of the United Kingdom to amount to an offence under this provision. This is the case regardless of whether the criminal law would require the offence, or any element of it, to take place in the United Kingdom (or a particular part of it)" (Ofcom's emphasis).

A1.30 Not every country or jurisdiction in the world prohibits the buying and selling of items covered by UK priority offences. We recognise the tension between protecting UK users from illegal content and the commercial interests of providers in hosting content (for providers of U2U services) or indexing search content (for providers of search services) for jurisdiction in which it is lawful. However, as we have explained above, the interpretative rule in the Act applies only to what happens in relation to the content. It does not affect, for example, any offline circumstances required for the offence to be committed. In the case of the buying and selling offences considered in the 'Drugs', and 'Weapons' sections, and having regard to the intention of Parliament, our view is that the words 'sale' and 'supply', and the linked phrase 'expose for sale' are best construed as relating to sale etc to persons in the UK. We do not consider it likely to be consistent with the intention of Parliament to suggest that all content should be considered legal unless it is expressly targeted at UK users. On the other hand, we also do not consider it practical to suggest that all over the world, overseas users and URL providers, should expressly state that UK users are not allowed to buy.

A1.31 We believe that there is no simple proxy by which service providers can infer that an exposure for sale etc. has potentially been made to UK users. We therefore consider that providers will need to make sensible, nuanced judgements on this point, having regard to the content itself, its context and – in particular – any evidence from users (via complaints) or from law enforcement that goods are being marketed unlawfully to users in the UK. If a piece of content explicitly or implicitly excludes UK consumers from its customer base, it follows that it cannot be said to amount to illegal content. If a piece of content makes it clear that the item in question may only be purchased in person in a location within the jurisdiction where it is legal, or if it makes clear that delivery to a buyer is restricted to those within the same jurisdiction, then we proposed that the buying and selling priority offences have not been engaged.

Drugs and psychoactive substances

Drugs

A1.32 In preparing our guidance on illegal content relating to offers to supply drugs and psychoactive substances, we considered whether it would be appropriate to identify drugs only by their legal (chemical) names and to make it the responsibility of service providers to keep their moderators up to date on the drugs' 'street names'. We recognise that street names used by dealers and drug users change often and so any list compiled by Ofcom would risk being incomplete and quickly outdated. We would not want Ofcom's guidance to be an excuse for service providers to fail to take appropriate steps to keep their knowledge of drugs slang properly up to date.

A1.33 However, our view is that the ICJG is for all service providers – including smaller service providers based overseas – and that a potentially incomplete list of drugs' street names is therefore better than no list. We have therefore drafted on that basis.

Offering to supply

A1.34 The priority drugs and psychoactive substances offences relate to the unlawful supply, or offer to supply, of controlled drug or psychoactive substances respectively. 'Offer' here takes its natural meaning in English rather than its technical meaning in the law of contract. We considered whether we could provide more guidance than that in our Illegal Content Judgement Guidance, but have concluded that – absent judicial authority – we would risk misdirecting providers by doing so.

A1.35 By its nature, an offer to supply must be made intentionally. Therefore, if the content amounts to an offer, the service provider will have reasonable grounds to infer that the state of mind requirements are met. We therefore do not discuss state of mind separately in our guidance.

Exemptions

A1.36 In the ICJG, we make reference to the Misuse of Drugs Regulations 2001 (SI 2001/3998) ('Misuse of Drugs Regulations 2001'). The regulations provide certain exemptions from the provisions of the Misuse of Drugs Act 1971. In some cases, these regulations are relevant to offering to supply controlled drugs and drugs article. It is our view that providers of U2U services will not encounter examples of exempted content on their services. However, we

recognise that it may be more challenging for search service providers to distinguish between illegal content and content which is legal due to the circumstances of its posting being exempted under the Misuse of Drugs Regulations 2001. We therefore conclude that, where providers of search services encounter content which could possibly to be exempted under the Misuse of Drugs Regulation 2001, they should take a pragmatic view, considering the context available and consider whether the controlled drugs appear to be sold in the UK.

Weapons offences

Firearms

What is a firearm?

A1.37 For the purpose of the ICJG, we focus on priority firearms offences from the Firearms Act 1968 (the "Firearms Act"). This is because they are the most comprehensive set of priority offences, differ only in minor technical detail from the equivalent Northern Irish legislation (Firearms (Northern Ireland) Order 2004 (S.I. 2004/702 N.I.3)) and advisors are likely to be more familiar with the Firearms Act because it applies to a greater territory. It is difficult to find a term that is clear about the weapons this Act covers. It includes 'firearms' as the Act defines them, but it also includes other weapons that it defines as not being firearms – for example air weapons. It also includes component parts and ammunition. Within the definition of firearms there are a number of types of weapon that a layperson may not intuitively consider to be 'firearms'; for example, pepper sprays, stun guns (often known by a brand name, tasers), and rocket launchers. In this statement, we use 'firearms' broadly, to cover all the types of weapon, parts and ammunition that are subject to the Firearms Act. In the ICJG specifically, we have provided guidance in such a way as to avoided providers having to grapple with the detail of what type of firearm they are considering unless it is absolutely necessary. This is due to the technical complexity of the matter at hand, and the likelihood that content moderators will lack a detailed specialist understanding of types of guns.

Sale or exposure for sale and structure of our guidance

A1.38 Most of the priority firearms offences in schedule 7 of the Act relate to the actual sale or purchase of the firearm concerned. However, such a transaction almost certainly takes place offline (for example, with the exchange of money) and cannot take place through the posting of user-generated content on a U2U service or in search content. What takes place online, either on a U2U service or in search content, is almost always only the lead-up to a sale or a purchase rather than the purchase itself. It is the marketing and advertising or 'exposure for sale' which encourages a potential buyer to contact a potential seller. We note that one priority offence for firearms, section 3 of the Firearms Act, relates to the activity of 'exposing for sale', and the ICJG therefore focuses on this. The offence in question takes place when a person who is not legally permitted to, exposes a relevant firearm for sale *by way of trade or business*. This offence applies to most types of firearm; however, there are exceptions, so we believe it is necessary to consider each offence in turn. In order to make these complex offences more understandable for a non-specialist audience, we have written the ICJG section on firearms as a series of questions.

Approach to 'by way of a business or trade'

A1.39 While the section 3 Firearms Act offence covers almost all types of firearms, the phrase 'by way of a trade or business' means that we believe that – in practice – it is appropriate for our guidance to distinguish between certain types of firearms. This is because the Firearms Act creates a class of weapons, 'prohibited weapons', which it is unlawful even to possess in the UK without specific authority from the Secretary of State in England and Wales and Scottish Ministers in Scotland. Such authority is normally only granted to those with a legitimate commercial need to possess prohibited weapons, rather than for private use or speculative business interest. It follows that a person dealing in such weapons lawfully will, by definition, be trading a business asset.

A1.40 The limits on lawful possession and trade of 'prohibited weapons' are likely to make it difficult for any person to acquire such weapons for unlawful onward sale. These are not the sort of weapons which it is likely that a casual seller might find in an attic and decide to place for sale online. Usually, it would take effort and knowhow which may be associated with fairly significant expense. The offence is also serious - possession of such items for sale is subject to a statutory minimum term of imprisonment of 5 years. Altogether, for these reasons, we consider it unlikely that a person in the UK dealing in such weapons unlawfully would be in a position to do so other than by way of a generally unlawful trade or business of some kind. The likelihood is therefore that 'prohibited weapons' are being dealt by way of an (unlawful) trade or business, and it is reasonable for providers to draw this inference.

A1.41 We note that the same is not true for less heavily restricted firearms that are not 'prohibited weapons', such as shotguns, air weapons and 'lethal barrelled weapons.' For these type of weapons, we have concluded that positive evidence would be needed to make a reasonable inference that trading in the UK was taking place by way of trade or business. It will therefore be reasonable to infer that trading was taking place by way of trade or business only if:

a) the person's account or website appears to be a marketplace containing multiple items for sale;
b) the person is holding themselves out as acting by way of a trade or business, for example by describing themselves as a professional, a gun trader or as doing business, or is using a company or business name; and
c) a sufficiently expert third party provides evidence that the person is acting by way of a trade or business.

Authorisation

A1.42 We note that there is no central, public or easily consulted register of which persons are authorised to deal in firearms in the UK. However, we understand that authorised dealers behave in ways which are likely to make unlawful sales identifiable to service providers. In particular, a website purporting to sell directly and remotely to UK users would not be authorised.

3D printing of firearms

A1.43 The Firearms Act does not cover 3D printing instructions for guns. However, we consider that in practice this type of content would be caught by one of the priority offences in schedule 5 of the Act. The offence in section 54 of the Terrorism Act 2000 relates to 'providing weapons training'. This covers providing instruction or training in the making of

firearms, making it available either generally or to one or more specific persons, and there is no state of mind requirement. Jurisdictional considerations play no part in this analysis. A defence is available if the user concerned can prove that their action or involvement was wholly for a purpose other than assisting, preparing for or participating in terrorism. We have concluded that this is likely to be difficult to show in relation to content circulated on the internet in places readily accessible to the general public.

Knives and 'offensive' weapons

A1.44 A disparate set of weapons are caught by the legislation relating to knives and offensive weapons: section 1 of the Restriction of Offensive Weapons Act 1959; Article 53 Criminal Justice (Northern Ireland) Order 1996 (S.I. 1996/3160 (N.I. 24) (flick knives and gravity knives); and section 141(1) of the Criminal Justice Act 1988 (offensive weapons). We consider that these are fairly straightforward offences which apply to any exposure for sale and do not have any state of mind requirements. Acknowledging the jurisdictional issues discussed above, we believe that the main challenge arises in correctly identifying the weapon itself and have therefore listed the weapons themselves and also provided a description of them, which is taken from UK government guidance.

A1.45 However, these offences are also subject to a series of defences which may be important for the creative, historical and religious sectors. At time of preparing this Statement, we have little evidence of how these defences are applied in practice or what effects are likely to follow from the way in which the Act defines illegal content. Nor do we have evidence of the risk of gaming by bad actors as a result of the content of our guidance. We also do not have discretion to change the definition of illegal content which is set by the Act, and can only set out the basis upon which we consider it reasonable for a service to infer that a defence exists.

A1.46 In the guidance on the relevant offences, we set out the available defences which we believe are relevant. We think that the online context makes it unlikely for the defence to arise that marketing is carried out only for the purposes of functions carried out on behalf of the Crown or of a visiting force. We have included that defence in the annex to the ICJG, but not within the main body.

'Marketing' and 'buying' offences

A1.47 A separate offence exists in section 1 and 2 of the Knives Act 1997 for the marketing of otherwise lawful knives in a way which indicates, or suggests, that the knife is suitable for combat; or is otherwise likely to stimulate or encourage violent behaviour involving the use of the knife as a weapon. This offence is defined in the legislation in substantial detail, and we refer providers to guidance published by the UK's Crown Prosecution Service for examples of how it may manifest in practice.

A1.48 In addition, a large number of the priority offences relating to weapons are not absolute prohibitions, but partial prohibitions. It is lawful to trade in weapons, but (where relevant) the buyer must be appropriately authorised, the right age, and not a criminal. The actual sale takes place offline, and so in considering these offences, the offences of encouraging, assisting and conspiracy are more likely to be relevant. However, a person cannot encourage, assist or conspire with themself. The user responsible for the content is not the same person as the person committing the main offence. The jurisdictional issues considered above mean, in addition, that the content is unlikely to be illegal content unless

there are reasonable grounds to infer that the user responsible for the content was aware that the purchase or sale itself would take place in the UK.

A1.49 We have grouped these offences together based on the nature of the offence and the nature of the buyer. We have based this on the argument that – notwithstanding that it is likely to be difficult of service providers to identify individual items of illegal content – they will still need to consider the risk of such illegal content being present, and providers of U2U services will also need to consider the risk that they will be used to facilitate the commission of these offences.

Image-based adult sexual offences

Extreme pornography

A1.50 Because the extreme pornography is a 'possession' offence, knowledge of the content of extreme pornography images is not required – the statutory defences deal with that. Knowledge that the person has uploaded an image is required; however, we think it is reasonable for service providers to infer this.

Human torture and animal welfare

The animal cruelty offence

A1.51 At a fairly late stage, the offence in section 4(1) of the Animal Welfare Act 2006 (unnecessary suffering of an animal) was added to Schedule 7 of the Act, to make it a priority offence. In this document, we refer to this offence as the 'AWA 2006 offence'. A person commits this offence where they know or ought reasonably to know that their conduct would cause, or would be likely to cause, unnecessary suffering to a protected animal.[327]

A1.52 The AWA 2006 which requires a person to commit an action that would cause, or would be likely to cause, unnecessary suffering, cannot itself be committed in the form of content. In other words, although online content can clearly depict an act of animal cruelty that would amount to an offence, the content cannot itself cause suffering to an animal. On the face of it, this means that there appears to be a risk that, taken in isolation, the priority AWA 2006 offence does not deal with pre-recorded animal cruelty in a suitably robust way.

A1.53 For this reason, our guidance also includes guidance on the offence of misuse of a public communications network (s.127(1) of the Communications Act 2003).

Approach to s.4(1) of the Animal Welfare Act 2006

Which animals and which suffering?

A1.54 The definition of the kinds of animals caught by the AWA 2006 offence is "An animal of a kind commonly domesticated in the British Islands, or an animal under the control of man (whether on a permanent or temporary basis) or an animal not living in a wild state". We have included this in full in the detailed legal annex, but for the purposes of the main

[327] The definition of 'protected animal' is detailed and it is not necessary to think about it in detail except when considering whether a specific item of content relates to a protected animal.

guidance document we consider that content moderators within the UK may find this test too hard to understand. Not even all those based within the UK would find it easy to say what amounts to 'domestication', what exactly the 'British Islands' are, or which animals are commonly domesticated. We think it appropriate to provide simplifications of the wording and a series of examples of types of animal and types of situations we consider would be caught.

A1.55 We have therefore decided to explain that unnecessary suffering may be of a physical or mental nature and may arise from a person's action or their inaction.

Jurisdiction

A1.56 In the case of the encouraging, assisting, and conspiring offences, the AWA 2006 offence being encouraged, assisted, or conspired to etc would need to be an offence which was somehow within the territorial jurisdiction of the UK courts. However, the precise rules the UK courts apply to determine whether they have jurisdiction over cases are, in our view, too complicated and require too much knowledge of UK laws for there to be any prospect that even a very well-resourced service provider would be able to apply them in practice. However, there are many scenarios in which the conduct would not amount to an offence of animal cruelty. We do not think it is possible for us to say it is reasonable for a service provider to infer the conduct to be an offence in every case (though a service may choose to do so, in an exercise of its own right to freedom of expression).

A1.57 We have therefore decided on a broad brush approach. We state that services have reasonable grounds to infer that the conduct amounts to an offence where there are reasonable grounds to infer that:

a) The AWA 2006 offence concerned takes place in the UK; or
b) Is to be committed by someone who is British; or
c) Is taking place in any other country where animal cruelty is an offence.

We consider that this approximates the rules a UK court would apply in a way that is understandable for service providers.

State of mind

A1.58 The offences of encouraging, assisting and conspiracy can only be committed with the right state of mind. For encouraging and assisting, that is intent or belief that an AWA 2006 offence will be committed (or that one of a number of offences, of which animal cruelty is one, will be committed). For conspiracy, that is intent that an AWA 2006 offence will be committed.

A1.59 However, a service provider will not be in a position to interview the user concerned about their state of mind. For the conduct element of 'encouragement' and 'assistance' the circumstances must be such that there is a possible offence to be encouraged or assisted, and for conspiracy there must be an agreement of some kind. We consider that once it is reasonable to infer that the conduct of the user is such as to encourage or assist animal cruelty to take place in real life, or that there really is an agreement to commit animal cruelty, it is reasonable based on the same information to infer intent or belief. We therefore do not consider this aspect of state of mind separately in our guidance.

A1.60 However, it is necessary for it to be reasonable to infer that the user concerned either knows or reasonably ought to know that the animal is experiencing physical or mental suffering. This requires us to take a view on what it is reasonable to say a user should

know. We have set out the circumstances in which we believe it is reasonable to assume knowledge in paragraph [15.19] of Chapter 15 on 'Animal cruelty.'

A1.61 We recognise that it may protect animals better from harm if services chose to take action against all content in which a user's conduct may mean animals are caused unnecessary suffering, even where the person causing it is unaware of that. However, Ofcom only has the powers given to us under the Act.

Approach to s. 127(1) of the Communications Act 2003

A1.62 For the reasons set out in Volume 3, Chapter 2 paragraphs 2.58 to 2.69, we have decided to provide guidance on Section 127(1) of the Communications Act 2003. The s. 127(1) offence is a non-priority offence that makes it an offence to:

a) Send by means of an electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
b) Cause any such message or other matter to be so sent.

A1.63 In order to be guilty of an offence under s. 127(1) the defendant must either have intended that the content be grossly offensive or of an indecent, obscene or menacing character, or must be aware that it could be taken to be so by a reasonable member of the public.[328]

A1.64 We have decided to focus on the on the 'obscene' content element, and not other aspects of the s. 127(1) offence, because we think the risks to freedom of expression to be very high even with guidance. This is because the terms used in the offence are too broad and so have a high risk of being misunderstood by those who are not experts in UK laws.

A1.65 We also consider the 'grossly offensive', 'menacing' or 'indecent' elements of the s.127(1) offence overlap with other priority offences. Parliament chose to define certain offences as priorities. We do not consider it proportionate at this early stage in the establishment of the regulatory regime for us to say that service providers should build their systems and processes so as to enable them to consider all potentially relevant non-priority offences as well as priority offences, where a priority offence already exists targeting the type of content concerned.

A1.66 We emphasize that 'obscene' in this context does not mean 'pornographic'. Pornography is not illegal. We are focusing on obscenity in its sense of content being atrocious or very horrific. However, it will be necessary to give very clear guidance to service providers in order to ensure that it is sufficiently clear that public interest content such as journalism exposing wrongdoing is not illegal content. It is not illegal to expose atrocities. Our guidance explains that for content to be obscene it must be more than just shocking, offensive or disturbing.

A1.67 We note that, even when narrowed down, this offence is vague and there is very little case law on it. It has the potential to be applied by service providers in a way which has very significant negative impacts on the right to freedom of expression, because the words used in it are capable of such broad interpretation. We recognise that this is a risk which is likely to be exacerbated by our inclusion of this offence in our guidance even in the narrow way we are proposing. However, if we do not explain in our guidance why pre-recorded 'real' torture videos amount to illegal content under the Online Safety Act, we consider there

[328] Following *DPP v Collins* [2006] UKHL 40, *DPP v Kingsley Smith* [2017] EWHC 359 (Admin).

would be a gap in our regulatory products which itself risks allowing serious harm to users to continue.