1. Our approach to developing Codes measures

The Online Safety Act places a new duty of care on online service providers to protect their users from harm and to place safety by design at the heart of their platforms. Ofcom's Codes of Practice (Codes) are one of the main tools we have to get providers to make improvements in these areas.

The measures in our Codes will result in change in three key areas:

- stronger safety governance and risk management;
- specific changes to design to improve safety; and
- increased choice for users so they can control their online experiences.

This chapter gives an overview of how we have approached developing this first edition of the Codes. It also addresses a number of key cross-cutting issues where we have had feedback to our consultations, and signals where further information on these may be found in the documents.

1. We have prioritised introducing the Codes as soon as possible to protect users

As we explain in our Register of Risk, illegal online content is widespread and causes significant harm. Given the scale and urgency of the challenge, it is important for us to make the Codes enforceable as soon as possible so that we can drive compliance and act against breaches at the earliest opportunity. Parliament set Ofcom a deadline of 18 months after the Act achieved Royal Assent for the first two phases of work to be completed, and we launched our first consultation, on illegal harms, less than two weeks from the Act passing.

As part of our Consultation we received suggestions for several new measures to the Codes. Where we were able to incorporate these because we already have sufficient evidence, we have done so. For measures where we need to do more assessment and gather further evidence, we have decided to launch a further consultation in the Spring of 2025. We have removed some measures from smaller low risk services, where the evidence we received suggested they were not proportionate.

Online safety is extremely dynamic, with harms, technology and best practice in user safety evolving quickly. This iterative approach to the Codes – banking what we already have, and building further over time – is central to our approach now and in the future.

2. We have taken a risk-based approach to our Codes

Our key focus is the extent to which measures can reduce risks to users. The Act requires us to ensure measures are proportionate, and we recognise that the size, capacity, and risks of services differ widely. We therefore do not take a one-size-fits-all approach. Instead, we have set out what types of service we think should use specific safety measures to comply with their duties, with the most extensive expectations on the riskiest services.

The size of a service and its user base is one indicator of risk. But there are some services which are inherently risky even when their reach is small. We are clear in our Codes that all providers of high-risk services must take robust steps to protect people, whether they are small or large.

Our Risk Assessment Guidance explains that providers should assess whether they are high, medium or low risk for each harm. The measures the Codes recommend vary depending on the outcome of this assessment. In general, the Codes recommend more onerous measures for high-risk services than for low-risk services. Consistent with this risk-based approach, we have chosen to apply a number of the most robust measures in our Codes to high-risk services even where they are small. This includes the measures on grooming and the measures relating to the detection of CSAM.

At the same time, it is reasonable to expect more of the largest providers than of smaller providers. We have in some cases imposed significant obligations on large low-risk providers because of their greater resources and reach. However, we have sought to minimise the regulatory burden on small low-risk services.

3. We have included a mix of cross-cutting and harms-specific measures in Codes

Many of the design changes will address multiple risks. In other cases, specific changes will address particular harms. Our Codes therefore include:

- A series of measures focused on governance - taken together with our risk assessment guidance these are intended to embed the building blocks of good risk management in providers;
- A series of cross-cutting measures, for instance content moderation measures, which look to ensure that a broad range of service providers take important actions that will address all illegal harms; and
- Some harm-specific measures which aim to address in a targeted way some of the most serious harms online, including child sexual abuse material (CSAM), grooming, terror, and fraud.

The Codes represent a package of measures which we recommend that service providers should take to comply with their duties under the Act. The Act stipulates that the Codes are a 'safe harbour'. This means that Ofcom must treat providers who choose to implement all applicable measures as complying with their relevant duties under the Act. The measures in our Codes are required by the Act to be clear and sufficiently detailed for providers to understand what they entail in practice.

What this chapter does

1.1 This chapter outlines the approach we have adopted to developing our first set of measures for the Illegal Content Codes of Practice ('Codes'). It also responds to key stakeholder feedback on our approach and cross-cutting elements of our work on Codes.

1.2 The chapter describes the purpose of the Codes as outlined in the Online Safety Act 2023 ('the Act') and then discusses the following aspects of our approach:

a) our strategy for the first iteration of the Codes;
b) our approach to the impact assessment of measures in the Codes; and
c) who the measures in our Codes apply to.

Purpose of Codes of Practice

1.3 The Act places a requirement on us to prepare and issue the Codes – a package of measures recommended for service providers to comply with their safety duties under the Act.

1.4 The Act says the Codes are like a 'safe harbour', meaning that service providers who choose to implement all applicable measures in the Codes will be treated as complying with their relevant duties under the Act.

1.5 This Illegal Harms Statement ('Statement') details the measures that we recommend service providers should implement to be compliant with the following legal duties:

a) illegal content safety duties contained in the Act (sections 10 and 24);
b) content reporting duties that relate to illegal content (sections 20 and 31);
c) duties relating to complaints procedures, apart from the parts of the duties which are only relevant to services likely to be accessed by children or Category 1 services (sections 21 and 32).

1.6 The Act stipulates that Codes measures should provide a sufficiently clear and detailed description of the actions we recommend service providers should implement in order to comply with their legal duties.

1.7 Service providers do not need to follow our Codes and may seek to comply with their safety duties by taking what the Act calls 'alternative measures'. Where providers take alternative measures, they must keep a record of what they have done and explain how the relevant safety duties have been met. The Act provides that, in doing so, they must consider the importance of protecting users' rights to freedom of expression within the law and of protecting users from breaches of relevant privacy laws. We set out what providers should record when taking alternative measures in our Record-Keeping and Review Guidance.

1.8 Under the Act, we are required to prepare and issue the following sets of Codes for 'Part 3 services'. These are for user-to-user (U2U) and search services. The Codes include:

a) a Code covering terrorism content (relating to the offences set out in Schedule 5)
b) a Code covering CSEA (child sexual exploitation and abuse) content (relating to the offences set out in Schedule 6)
c) one or more Codes for the purpose of compliance with other relevant duties (including but not limited to those relating to the offences set out in Schedule 7)

1.9 Together these Codes cover all the kinds of illegal harm as captured under the Act.

1.10 As stated in our November 2023 Illegal Harms Consultation ('November 2023 Consultation'), we have produced two documents. One document contains measures applicable to U2U services and one document contains measures applicable to search services. Each document combines the terrorism Code, CSEA Code and other duties Codes mentioned in paragraph 1.8. We have combined the Codes in this way to assist service providers. Providers do not need to know whether measures are in the terrorism Code, CSEA Code or other Codes. Rather, providers can consult the two documents, which detail measures applicable to them.

Ofcom's strategy for first iteration of Codes

Our November 2023 Illegal Harms Consultation

1.11 In the November 2023 Consultation, we proposed initial measures that would make a real difference to users in the UK. We set out that our first iteration of Codes would create a strong foundation on which to build over time.

1.12 Through the measures in our Codes we are aiming to make everyone's life online safer, particularly children. In some cases, we do that by pushing service providers across the industry to improve standards. In other cases, we do that by codifying things that some of the providers are already doing and pushing other high risk service providers to adopt these practices.

1.13 Our Codes include:

a) **A series of measures focused on governance**- taken together with our risk assessment guidance these are intended to embed the building blocks of good risk management in providers; [1]
b) **A series of cross- cutting measures** which look to ensure that a broad range of service providers take important actions that will address all illegal harms; and
c) **Some harm-specific measures** which aim to address in a targeted way some of the most serious harms online, including child sexual abuse material (CSAM), grooming, terror, and fraud.

Stakeholder feedback[2] [3]

General approach

1.14 A number of stakeholders endorsed our approach and intention in developing our first Codes and the different types of measures recommended.[4] [5] Stakeholders endorsed most of the measures we proposed.[6] We received some support for our approach in responses

[1] Which were part of a wider package inclusive of our risk assessment guidance.
[2] Note this list in not exhaustive, and further responses can be found in Annex 1.
[3] Ofcom has also had careful regard to advice received from our Advisory Committees.
[4] Association of Police and Crime Commissioners response to November 2023 Illegal Harms Consultation, p.4; British and Irish Law Education Technology Association (BILETA) response to November 2023 Illegal Harms Consultation, p.5; Centre For Competition Policy (CCP) response to November 2023 Illegal Harms Consultation, p.16; Children's Commissioner for England response to November 2023 Illegal Harms Consultation, p.21; Cyber Helpline response to November 2023 Illegal Harms Consultation, p.8; Dwyer, D. response to November 2023 Illegal Harms Consultation, p.4; Global Network Initiative response to November 2023 Illegal Harms Consultation, p.8; Google response to November 2023 Illegal Harms Consultation, p.1; Independent Inquiry into Child Sexual Abuse (IICSA) Changemakers response to November 2023 Illegal Harms Consultation, p.3 Internet Watch Foundation (IWF) response to November 2023 Illegal Harms Consultation p.9; LinkedIn response to November 2023 Illegal Harms Consultation, p.8; Meta response to November 2023 Illegal Harms Consultation, p.15; Mid Size Platform Group (MSPG) response to November 2023 Illegal Harms Consultation, p.5; [✂]; National Trading Standards eCrime Team response to November 2023 Illegal Harms Consultation, p.6; Segregated Payments Limited response to November 2023 Illegal Harms Consultation, p.6; South East Fermanagh Foundation response to November 2023 Consultation, p.6; Stop Scams UK response to November 2023 Illegal Harms Consultation, p.9; WeProtect Global Alliance response to November 2023 Illegal Harms Consultation, p.8
[5] We note that a large number of respondents did not set out a view on our approach to the Codes.
[6] We set out the individual feedback to the proposed measures in the relevant chapters.

to our May 2024 Consultation on Protecting Children from Harms Online ('May 2024 Consultation').[7]

1.15 However, there were a number of areas where respondents raised significant concerns.

1.16 The Online Safety Act Network (OSA Network) considered that we had not consulted on our underlying approach, and expressed concern that the overall approach would not be iterated upon in future.[8] [9]

Safe harbour

1.17 Some respondents expressed concern that the 'safe harbour' concept could result in perverse incentives for service providers when it comes to user safety. For example:

- Several service providers argued that the provision could or would lead to unnecessary or even counterproductive changes being made to services to ensure compliance.[10]
- Others were concerned that service providers would not be incentivised to offer protections beyond the scope of the Codes, including innovative measures, which could lead to them potentially rolling back existing systems and thus fail to achieve the intentions of the Act.[11] [12]

---

[7] Association of Police and Crime Commissioners response to May 2024 Consultation on Protecting Children from Harms Online, p.10; Centre for Excellence for Children's Care and Protection (CELCIS) response to May 2024 Consultation on Protecting Children from Harms Online, p.11; Google response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Microsoft response to May 2024 Consultation on Protecting Children from Harms Online, p.8; MSPG response to May 2024 Consultation on Protecting Children from Harms Online, p.7; National Crime Agency (NCA) response to May 2024 Consultation on Protecting Children from Harms Online, p. 17; Pinterest response to May 2024 Consultation on Protecting Children from Harms Online, p.8;

[8] Online Safety Act Network (OSA Network) response to November 2023 Illegal Harms Consultation, p.4. We note that the OSA Network 2 made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.10. Each Consultation asked a question about our approach to developing Codes of Practice (see Q12 in the November 2023 Consultation and Q25 in the May 2024 Consultation).

[9] We set out the OSA Network's specific concerns regarding our approach in paragraph 1.20 below.

[10] Airbnb response to November 2023 Illegal Harms Consultation, p.15. Airbnb argued that, if the requirements of the Code of Practice are too prescriptive, the safe harbour provision may lead to service providers following the recommended measure to ensure compliance, rather than considering whether an alternative, more robust, and more effective approach could be taken and investing in that approach. Booking.com response to November 2023 Illegal Harms Consultation, p. 19; Meta response to November 2023 Consultation, p.16; Reddit response to November 2023 Illegal Harms Consultation, pp.4-5.

[11] Airbnb response to November 2023 Consultation, p.15; Barnardo's response to November 2023 Illegal Harms Consultation, p.10. We note Barnardo's made a similar point in response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Booking.com response to November 2023 Consultation, p.19; Center for Countering Digital Hate (CCDH) response to November 2023 Illegal Harms Consultation, pp.8-9; Children's Commissioner for England response to May 2024 Consultation on Protecting Children from Harms Online, p.46; Christian Action Research and Education (CARE) response to November 2023 Illegal Harms Consultation, p.9; [✂]; IWF response to November 2023 Illegal Harms Consultation, pp.16-17. We note that IWF made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.4; Molly Rose Foundation response to November 2023 Illegal Harms Consultation, p.4. We note that the Molly Rose Foundation made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.11; National Society for the Prevention of Cruelty to Children (NSPCC) response to November 2023 Illegal Harms Consultation, p.14; OSA Network response to November 2023 Consultation, p.62. We note that the OSA Network made a similar point in its response to the May 2024 Consultation, p.43.

[12] We address the points regarding providers not having to tackle all of the risks identified in their risk assessment from paragraph 1.19.

- There were concerns from respondents about penalties associated with taking alternative measures. TechUK and Google expressed concern that service providers would be penalised for taking other measures, and Meta argued that we should offer more than one way for a service to be within the safe harbour for a particular measure.[13] [14]

1.18 Some stakeholders also asked for more guidance to services on how to take alternative measures.[15]

Oversight and management of risks identified

1.19 Several civil society organisations noted a concern that, because the Codes are a safe harbour, providers that followed the Codes would be deemed compliant even if they did not put in place effective mitigations for all the risks identified in their risk assessment.[16] They considered this to be the case due to the absence of a mechanism in place to ensure that services manage all risks identified in their risk assessments. A number of these stakeholders argued that this was fundamentally antithetical to the aims of the Act.

1.20 To address this concern, the OSA Network suggested we introduce an additional measure recommending all service providers address all risks identified in their risk assessments, particularly those arising from features and functionalities.[17] In the absence of further efforts to strengthen our Codes, the OSA Network felt this would help achieve the safety by design intent of the Act by ensuring all potential risks would be overseen and accounted for by service providers.[18]

1.21 In a related point, some stakeholders questioned the link between the Register of Risks ('Register') and the Codes and asked why some harms or risks did not have proposed mitigations.[19]

---

[13] Google response to November 2023 Consultation, p.31; techUK response to November 2023 Illegal Harms Consultation, p.17.

[14] Meta (response to November 2023 Consultation, p.16.

[15] Association of Police and Crime Commissioners response to November 2023 Consultation, p.4; Pinterest response to November 2023 Illegal Harms Consultation, p.4. We note that Pinterest made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.5; techUK response to November 2023 Consultation, p.18.

[16] This includes the following stakeholders, please see Volume 1: chapter 5 'Governance and accountability' for further responses: Children's Coalition for Online Safety response to May 2024 Consultation on Protecting Children from Harms Online, p.2; OSA Network response to November 2023 Consultation, p.62; OSA Network Violence Against Women and Girls (VAWG) Sector Experts Response to May 2024 Consultation on Protecting Children from Harms Online, p.4.

[17] OSA Network response to November 2023 Consultation, p.18.

[18] Section 1(3) of the Act.

[19] 5Rights Foundation response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Barnardo's response to November 2023 Consultation, p.10-11. We note Barnardo's made a similar point in response to May 2024 Consultation, pp.6-7; CCDH response to November 2023 Consultation, p. 2. We note that CCDH made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.2; Children's Coalition for Online Safety response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Children's Commissioner for England response to May 2024 Consultation, p.38; Clean Up The Internet response to November 2023 Consultation, p.1; Global Action Plan response to May 2024 Consultation on Protecting Children from Harms Online, p.2; IWF response to May 2024 Consultation, p.4; Logically response to November 2023 Illegal Harms Consultation, p.9; Marie Collins Foundation response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Molly Rose Foundation response to November 2023 Consultation, p.29. We note that the Molly Rose Foundation made a

Package of measures

1.22 Many respondents argued that there were gaps in our proposed measures. A number of Civil society organisations noted concerns that our approach had set the bar too low for the first measures and that the proposed package was not substantial enough to impact online harms.[20] They suggested a large number of additional measures we could propose, which covered the breadth of harms captured under the Act, various different types of services, and protections for different user groups or for specific harm areas. This includes a number of responses calling for additional measures to address the heightened and distinct risk of harm to women and girls online.[21] A small number of service providers also noted measures they were already taking for which we did not have equivalent proposals.

1.23 Many civil society organisations considered that we needed to implement their proposed additional measures quickly. Some noted concerns that because the harms were occurring now, we needed applicable measures sooner rather than later.[22]

1.24 The OSA Network argued that the novelty, complexity and speed of companies captured by the Act means that our approach will struggle to keep up with the emerging harms and innovations in technology.[23] In this context, they argued that treating the Codes as a safe harbour meant that the regulatory framework would struggle to keep pace with technological, market and societal change. They argued that the measure they proposed (see paragraph 1.20) would address this concern.

1.25 Other stakeholders emphasised the importance of iteration in line with our proposed approach. Some noted that an iterative approach was needed to ensure that the Codes

---

similar point in its response to the May 2024 Consultation, p.43; NSPCC response to May 2024 Consultation on Protecting Children from Harms Online, p.3; OSA Network response to November 2023 Consultation, pp.61-62; We note that the OSA Network made a similar point in its response to the May 2024 Consultation, p.7; Refuge response to November 2023 Consultation, p.8; UK Safer Internet Centre (UKSIC) response to May 2024 Consultation on Protecting Children from Harms Online, p.22; Violence Against Women and Girls (VAWG) Alliance response to May 2024 Consultation on Protecting Children from Harms Online, p.3; Vodafone response to May 2024 Consultation on Protecting Children from Harms Online, p.2.

[20] CCDH response to November 2023 Consultation, p.9. We note that CCDH made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.2; Clean Up The Internet response to November 2023 Illegal Harms Consultation, p.2; Community Security Trust response to November 2023 Consultation, p.3; [✂]; Molly Rose Foundation response to November 2023 Consultation, p.3. We note that the Molly Rose Foundation made a similar point in its response to the May 2024 Consultation, pp.1, 4; OSA Network response to November 2023 Consultation, pp. 4, 7. We note that the OSA Network made a similar point in its response to the May 2024 Consultation, p.11; Parenting Focus response to May 2024 Consultation on Protecting Children from Harms Online, p.36; Refuge response to November 2023 Illegal Harms Consultation, p.8; Samaritans response to May 2024 Consultation on Protecting Children from Harms Online, p.2; Victims' Commissioner for England and Wales response to November 2023 Illegal Harms Consultation, pp.8-9.

[21] Domestic Abuse Commissioner response to November 2023 Consultation, p. 5; EVAW response to November 2023 Consultation, p. 2; Glitch response to November 2023 Consultation p. 4; OSA Network response to November 2023 Consultation, p. 94; The Suzy Lamplugh Trust response to November 2023 Consultation, p. 9; South West Grid for Learning response to November 2023 Consultation, p. 4; Victim's Commissioner response to November 2023 Consultation, p. 8.

[22] Barnardo's response to November 2023 Consultation, p.2; End Violence Against Women Coalition (EVAW) annex response to November 2023 Illegal Harms Consultation, p.34; OSA Network response to November 2023 Consultation, p.31-34.

[23] OSA Network response to November 2023 Consultation, pp. 34-35. We consider this response further in section x on precautionary principle.

remain up to date.[24] For example, the National Society for the Prevention of Cruelty to Children (NSPCC) was broadly supportive of elements of our approach, but noted that our proposals needed to be more ambitious in future to avoid the risk of not protecting children online.[25]

Design of measures

1.26 We received several responses requesting that we take a different approach to the design and creation of measures.

Prescriptiveness of proposed measures

1.27 Several respondents considered that some of our proposed measures were too prescriptive.[26] A number noted that 'higher level' measures might offer them greater flexibility. Several also noted that a more prescriptive approach could result in the Codes not being 'future-proofed', leading them to become ineffective over time by not allowing for changes in industry, technology, or harms. Some further argued that a prescriptive approach was not consistent with the diversity of practice across regulated services.

1.28 Some of these themes and ideas were supported by civil society organisations, who warned of 'tick box' compliance and suggested it could limit innovation or lower industry standards.[27]

[24] Cyber Helpline response to November 2023 Consultation, p.8; Match Group response to November 2023 Illegal Harms Consultation, p.8; Meta response to November 2023 Consultation, pp.14-15; National Association of Head Teachers (NAHT) response to May 2024 Consultation on Protecting Children from Harms Online, p.17; [✂]; Oxford Disinformation and Extremism Lab (OxDEL) response to November 2023 Illegal Harms Consultation, p.8; Parenting Focus response to May 2024 Consultation on Protecting Children from Harms Online, p.8; National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) response to May 2024 Consultation on Protecting Children from Harms Online, p.13.

[25] NSPCC response to November 2023 Consultation, p.13.

[26] Center For Data Innovation response to November 2023 Illegal Harms Consultation, p.9; Google response to November 2023 Consultation, p.31. We note Google made a similar point in its response to the May 2024 Consultation, p.5; Meta response to November 2023 Consultation, p.1. We note Meta made a similar point in its response to the May 2024 Consultation, p.3; MSPG response to November 2023 Consultation, p.5; Name Withheld 3 response to November 2023 Illegal Harms Consultation, p.8; Pinterest response to November 2023 Consultation, p.4. We note Pinterest made a similar point in its response to the May 2024 Consultation, p.4; Reddit response to November 2023 Consultation pp.8-10; Roblox response to November 2023 Illegal Harms Consultation, p.13. We note that Roblox made a similar point in its response to the May 2024 Consultation on Protecting Children from Harms Online, p.14; TikTok response to May 2024 Consultation on Protecting Children from Harms Online, p.1.

[27] Barnardo's response to November 2023 Consultation, p.1, p.9; Christian Action Research and Education (CARE) response to November 2023 Consultation, p. 9; CCDH response to November 2023 Consultation, pp.8-9; Cifas response to November 2023 Illegal Harms Consultation, p.5; Clean Up the Internet response to November 2023 Consultation, p.3; Community security Trust and Antisemitism Policy Trust response to November 2023 Illegal Harms Consultation, p.2; Molly Rose Foundation response to November 2023 Consultation, p.30; OSA Network response to November 2023 Consultation, p.87.We note that the OSA Network made a similar point in its response to the May 2024 Consultation, pp.47-48; Suzy Lamplugh Trust response to November 2023 Illegal Harms Consultation, p.9. UKSIC response to May 2024 Consultation, p.27.

Safety by design

1.29 A number of stakeholders considered that we should recommend more measures around 'safety by design'.[28] These requests cover a broad spectrum of themes, which we outline in this section.

1.30 Several stakeholders argued that our measures focused on mitigating harm after it had taken place (which was characterised as a 'downstream' approach).[29] They requested we take a more 'upstream' safety by design approach, applying more preventative measures to protect users, particularly women and girls, before harm occurs.[30] The OSA Network requested that we give greater consideration to how services and products could be made safer during the design and initial testing stages.[31] It also suggested there would be benefits attached to a further measure on monitoring the effectiveness of mitigations.[32]

1.31 Several stakeholders considered that we should propose measures that specified desired outcomes, noting that this would be beneficial in contrast to a prescriptive approach.[33]

1.32 Some respondents felt that our proposed measures and our approach were overly content-specific.[34]

---

[28] 5Rights Foundation response to May 2024 Consultation, p.2; CCDH response to November 2023 Consultation, p.8; Community Security Trust response to November 2023 Consultation, p.2; Cybersafe Scotland response to November 2023 Illegal Harms Consultation, p.6; Frida response to November 2023 Illegal Harms Consultation, p.4; IWF response to November 2023 Consultation, p.14; [✂]; NSPCC response to November 2023 Consultation, p.14. We note that the NSPCC made a similar point in its response to the May 2024 Consultation, p.39; OSA Network response to November 2023 Illegal Harms Consultation, p.8. We note that the OSA Network made a similar point in its response to the May 2024 Consultation, pp.13-14; Samaritans response to November 2023 Consultation, p.2; Suzy Lamplugh Trust response to November 2023 Consultation, p.4; UKSIC response to November 2023 Illegal Harms Consultation, p.3. We note that UKSIC made a similar point in its response to the May 2024 Consultation, p.41;

[29] Alliance to Counter Crime Online response to November 2023 Illegal Harms Consultation, p.1; Christchurch Call Advisory Network response to November 2023 Illegal Harms Consultation, p.5; Domestic Abuse Commissioner's Office response to November 2023 Illegal Harms Consultation, p.7; Molly Rose Foundation response to November 2023 Consultation, p.30; NSPCC response to November 2023 Consultation, p.14; Yoti response to November 2023 Illegal Harms Consultation, p.13.

[30] End Violence Against Women Coalition response to November 2023 Illegal Harms Consultation, p.3; Refuge response November 2023 Consultation, p.8; Suzy Lamplugh Trust response to November 2023 Consultation, p.9; UKSIC response to November 2023 Consultation, p.21; Victim's Commissioner for England and Wales response to November 2023 Consultation, p.8.

[31] OSA Network response to November 2023 Consultation, pp.11-12.

[32] OSA Network response to November 2023 Consultation, p.19.

[33] 5Rights Foundation response to November 2023 Illegal Harms Consultation, p.2; CCDH response to November 2023 Consultation, p.8; Cifas response to November 2023 Consultation, p.5; Community Security Trust response to November 2023 Consultation, p.2; Frida response to November 2023 Consultation, p.4; Molly Rose Foundation response to November 2023 Consultation, p.7; Name withheld 3 response to November 2023 Consultation, p.8; NSPCC response to November 2023 Consultation, p.14. We note that the NSPCC made a similar point in its response to the May 2024 Consultation, p.22; OSA Network response to May 2024 Consultation, p.43; Pinterest response to November 2023 Consultation, p.4; UKSIC response to November 2023 Consultation, p.8.

[34] Domestic Abuse Commissioner's Office response to November 2023 Consultation, p.7; [✂]; Yoti response to November 2023 Consultation, p.13.

Our response: Ofcom's strategy for the Codes

Safe harbour

1.33 In creating the Codes, we are working within the framework of the Act, which is set by Parliament. While we can iterate our Codes, we cannot change what the Act requires of us.

1.34 The Act provides that compliance with the Codes is deemed compliance with the safety duty.[35] We therefore have no discretion over the 'safe harbour' status of the Codes.

1.35 In preparing the Codes, we are required to have regard to the principles that:

a) the measures contained must be sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice; and
b) the measures for each kind and size of service must be proportionate to our assessment of the risk of harm they present.[36]

1.36 If we were to set out Codes that were too 'general' or 'high level' (so that it would not be clear for a provider what it needs to do), this would be inconsistent with the intent of the Act. This presents difficulty then in regard to stakeholder requests for regulation and measures to address novel or emerging harms. We note, we have designed several measures to allow service providers flexibility and to make their own choices regarding how to best protect their users.

1.37 The Act provides flexibility for those who do not wish to adopt Codes measures to take alternative measures. We recognise that some providers would prefer to avail themselves of the safe harbour than to run any risk of non-compliance by adopting alternative measures. While we have sought to draft measures in a way which does not unduly constrain providers, in order to function as the Act requires, the Codes need to be clear and detailed enough for it to be possible to say whether or not a provider has implemented the recommendations they contain. As set out in our record-keeping guidance, providers who wish to take alternative measures are entitled under the Act to do so, provided that they record how this complies with the safety duty and their duties in relation to freedom of expression and privacy.

1.38 We recognise that there is a tension between describing measures sufficiently clearly for providers to know what it is they need to do, and leaving space within our Codes for innovation. Where we consider it is appropriate to define a clear outcome and leave it to providers to decide how to achieve the outcome, we have done so.

Oversight and management of risks identified

1.39 Codes set out the measures we recommend service providers follow to address their risks. We cannot include a generic measure that recommends service providers should remove all risks, as some stakeholders have suggested. The safety duties in the Act only require providers to take proportionate steps and we can only make recommendations we are satisfied are proportionate, having impact assessed them. We cannot assess the impact of a proposal if we do not know what compliance with it would entail.

1.40 It is also not possible within the framework of the Act to recommend a measure that asks a service to remove all risks where proportionate to do so. Such a measure would not be

[35] S.49(1) of the Act.
[36] Schedule 4 paragraph 2(b) and (d) of the Act.

consistent with the Act because it is not sufficiently clear or detailed enough for the provider to know what it needs to do to fall within the safe harbour.

1.41 The Act distinguishes between actions service providers need to take to assess their risks and the steps they need to take to mitigate risks. The suitable and sufficient risk assessment that all service providers are required to undertake should provide providers with a complete understanding of their risks. The governance and accountability measures in Codes complement the risk assessment duty. In response to the feedback to both Consultations, we have made amendments to our proposals which are intended to ensure there are formalised accountability, reporting and audit processes in place for activities related to managing risks (including risks remaining after implementing Codes of Practice), as identified in a service's risk assessment. For further details of these amendments, please refer to Volume 1: chapter 5: 'Governance and accountability'.

1.42 In addition, the content and search moderation and reporting and complaints measures both include recommendations that mean the provider should continue to use the findings of the service risk assessment when designing and implementing core parts of its policies. The provider should have regard to the service risk assessment when setting its internal content policies and when designing its systems and processes for enabling users to make relevant complaints.

1.43 The 'safe harbour' standing of Codes does not preclude services from taking additional measures beyond those in Codes. These could relate to actions that have been identified through their governance and accountability structures.

Design of measures

1.44 We have thought carefully about the design of our measures, and what is the right mix of specific, outcomes based, and more "general" formulations of measures.

1.45 We have taken a hybrid approach because we think there is no one correct type of measure, and the decision on which type of measure to recommend requires a degree of judgement from us having regard to the nature of the harm we are seeking to address. Furthermore, there are areas where our current evidence or understanding of proportionality has led us to recommend a certain type of measure at this stage in our work.

1.46 As a combined package, we consider that these measures will ensure effective protections for users. We have recommended the following types of measures.

- **Specific measures** – where we have clear evidence that a specific action is the best means of improving outcomes for users, and clarity on expectations is paramount. Relevant examples of this approach in our Codes are our CSAM hash-matching measures and some of our grooming measures. The more the technology used to address a specific harm is in flux, the less likely we are to recommend specific measures.
- **Outcomes-based measures** – where we are able to identify a sufficiently clear outcome, and where the method by which this is achieved is less important. A relevant example of this approach in our Codes is our measure which recommends search providers should take appropriate action in relation to illegal content they are aware of, that achieves the outcome of either the content no longer appearing in search results or being given a lower priority in search results.
- **General measures** – where the action the provider must take is specified in more general terms, giving the provider considerable flexibility over exactly how the measure

is delivered. Relevant examples of this approach in our Codes are our measures on tracking new and increasing illegal harms on a service, performance targets, and terms of service. While more general, these measures are still sufficiently clear about what a provider needs to do to fulfil its duties. We are more likely to recommend general measures when the technology available to address a specific harm is evolving and where the most appropriate implementation will vary among services.

1.47 We note that it is very difficult to define a measure that is purely specific or outcomes-based, and that these measures, along with more general measures, may well require a blend of approaches to be effective in tackling harm. Our measure recommending the removal of CSAM URLs on search services is an example of where we have used a combination of approaches.

1.48 We agree with stakeholders that the fundamental themes captured in their safety by design requests are important. We consider that there are several ways in which our existing package of measures asks for safety by design, for example:

- As described in Volume 1: chapter 5: 'Governance and accountability' we have included measures that aim to embed user safety within a service providers' decision making, and we consider this to be an important step toward protecting users from illegal harms;
- We set out in Volume 2: chapter 7: 'Recommender systems' our measure that means that in scope providers should, when carrying out on-platform testing of content recommender systems, collect additional safety metrics when making design adjustments;
- The measures discussed in Volume 2: chapter: 8 'U2U settings, functionalities, and user support' introduces design changes that will keep children safer online, by making it harder for unconnected adults to find and connect with them; and
- In Volume 2: chapter 12: 'User controls' measures will provide tools for users to enable them to better control their online experiences and limit unwanted interactions that could lead to harm.

1.49 We also consider that our full package of guidance and Codes further aids these aims. For example, as part of their risk assessments, services will need to undertake a 'suitable and sufficient' assessment of the risks on their services. The four-step process we have set out in our Risk Assessment Guidance will help providers to understand harms, assess risks, implement measures, and monitor and review impacts on their services. We consider these actions to be closely aligned with good safety by design principles.

1.50 We consider it appropriate that a number of our Codes measures relate to content, as the Codes flow from the duties in the Act that relate to illegal content. Furthermore, it is appropriate for services to consider content as an important principle of achieving safety; there is clear evidence of exposure to content leading to harm. Therefore, it would not be possible for a provider to comply with its duties if it had no ability to consider content.

Iterative approach

1.51 We have made the decision to move quickly to confirm and publish the majority of measures broadly as we proposed in our November 2023 Consultation.[37]

1.52 Our first iteration of Codes creates a strong foundation to build on over time.

1.53 Importantly, the duties on service providers do not come into effect until the Codes are in force. Delaying this package to consult on a more far-reaching package of measures would mean a delay to bringing in important protections for users, and there are important other benefits to going early including:

- In early 2025, providers will need to do their first 'suitable and sufficient' risk assessments under the Act and our governance measures will promote accountability and place managing online safety risk at the heart of providers decision making;
- It will raise the bar of protections, in particular for many users of smaller, medium-sized and riskier services; and
- It embeds important harm specific measures, particularly those that are aimed at protecting children, such as our CSAM hash-matching / URL detection and Grooming measures.

1.54 It will also enable us to start to enforce against deliberate or egregious breaches as soon as the duties come into effect, making a difference in relation to the highest priority harms rapidly.

1.55 We note that speed and having the most far reaching set of Codes are difficult to achieve in tandem. This is because it is a statutory regulatory process, the timeframe is short for a project of this scale and novelty, the work required to develop the Codes is highly complex and detailed, and we need to ensure that the measures we recommend are proportionate. This is made more challenging by the wide range of services in scope of the regime, many of whom are very small.

1.56 Nonetheless, regulated providers can expect that we will continue to raise the bar over time. Most immediately, we will set out proposals for some additional measures in our Spring 2025 Consultation. This will feature a range of potential measures, including but not limited to measures to ban those that share CSAM, Intimate Image Abuse Hash Matching to prevent the sharing of non-consensual imagery, and a broader automated content moderation measure. As noted above, a number of stakeholders have suggested additional measures that we could propose. We will continue to explore these and other potential measures as we plan and work towards future iterations of our Codes.

[37] We have made some minor changes, e.g. to clarify definitions and more precisely align our drafting with the Act, some of which affect all measures. We have also made some cross cutting changes which affect all or many measures because they relate to how we have defined who measures apply to. These are explained further in this chapter. In the rest of this Statement, when we talk about changes to a measure (including explaining whether and how it has changed) we do not rehearse these changes again unless they make a difference to our analysis of the proportionality of the measure. Stakeholders should therefore assume that these changes have also been made to our Codes, where relevant.

Our approach to assessing measures via our impact assessment framework

Our November 2023 Illegal Harms Consultation

1.57 In our November 2023 Consultation, we set out our proposed approach to the impact assessment of our recommended measures.

1.58 We stated that (1) our assessment could vary for different types of services, (2) that we considered carefully which services each measure should apply to, and (3) that a key element of our assessment was the proportionality of the measure.

1.59 We also explained that we undertook our assessment by looking at both the individual measures on their own merits and at the measures in combination.

1.60 There are some measures that closely reflect specific requirements in the Act, and which all service providers in scope of the safety duties must follow.[38] As the impacts from such measures are caused by the Act (rather than by how we have considered them), we did not carry out a detailed impact assessment of them.

Stakeholder feedback[39]

How we have assessed measures

1.61 Several stakeholders argued that our approach to proportionality placed undue emphasis on the economic burden to service providers and the impact on competition within the sector, rather than on the impacts of online harms on individuals and society.[40]

[38] For example, under section 10(5) of the Act, all services must ensure that they have Terms of Service which are inclusive of certain information. The Act requires services which do not currently have such Terms of Service to develop them; the benefits or costs of doing so are not a matter in relation to which we exercise any discretion in our Codes of Practice.

[39] Note this list in not exhaustive, and further responses can be found in Annex 1

[40] 5Rights Foundation response to November 2023 Consultation, pp.10-11, p.18; Barnardo's response to November 2023 Consultation, pp.14-15. We note that Barnardo's made a similar point in its response to the May 2024 Consultation, p.28; Bereaved Families for Online Safety response to November 2023 Illegal Harms Consultation, p.1; Canadian Centre for Child Protection (C3P) response to November 2023 Illegal Harms Consultation, p.12; CARE response to May 2024 Consultation on Protecting Children from Harms Online, p.7; CCDH response to November 2023 Consultation, p.11; Children's Commissioner for England response to May 2024 Consultation, p.40; Clean Up The Internet response to November 2023 Consultation, p.6; Community Security Trust response to November 2023 Consultation, p.2; End Violence Against Women Coalition response to November 2023 Consultation, p.2; Global Partners Digital response to November 2023 Illegal Harms Consultation, p.23; Institute for Strategic Dialogue response to November 2023 Illegal Harms Consultation, p.6; IWF response to November 2023 Consultation, p.3; Molly Rose Foundation response to November 2023 Consultation, p.31. We note that the Molly Rose Foundation made a similar point in its response to the May 2024 Consultation, pp.6-8; OSA Network response to November 2023 Consultation, pp.40-46, Annex B pp. 20-23; We note that the OSA Network made a similar point in its response to the May 2024 Consultation, p.37; NSPCC response to May 2024 Consultation, p.40; Samaritans response to November 2023 Illegal Harms Consultation, p4; We note that Samaritans made a similar point in its response to the May 2024 Consultation, p.3; Segregated Payments Ltd response to November 2023 Consultation, p. 15; UK Finance response to November 2023 Illegal Harms Consultation, p.15; UKSIC response to May 2024 Consultation, p.20.

1.62 One service provider asked for clarification on the proportionality of measures, asking for it to be made clear that providers would only be required to implement those solutions where it would be proportionate to do so.[41]

Costs

1.63 Some stakeholders raised concerns that our approach did not proportionately consider the opportunity costs where existing staff and resources may need to be reallocated from existing functions to work on the implementation of our recommended measures.[42]

1.64 One stakeholder raised concerns about our approach and asked that costs, benefits, and risk of harm be quantified for each measure.[43]

Rights

1.65 One stakeholder welcomed our approach to balancing rights but asked for more detail on safeguarding user's rights on the basis that the safeguards for freedom of expression, privacy, and data protection were both generally insufficient and inconsistent with the intention of Parliament.[44] Google asked that further consideration be given to users' rights to freedom of expression, highlighted concerns regarding impacts on users' right to privacy in several areas.[45]

1.66 The OSA Network said that we had failed to consider the rights of victims and had failed to consider rights other than freedom of expression and privacy.[46] Relatedly, a particular area of concern was that our approach might negatively impact the rights of vulnerable groups such as women and girls.[47] The OSA Network also raised a concern with our approach to minority languages in the UK, stating that while we noted our obligation to the Welsh language, the same was not done for other languages.[48]

1.67 The Oxford Disinformation and Extremism Lab (OxDEL) expressed concern about the impact that deplatforming and content removal could have on academics and researchers.[49] One stakeholder argued that service providers should be compelled to enforce freedom of expression and that we should focus on how their actions to mitigate illegal harms may influence their treatment of user expression (the limitation of which is also a harm).[50] A

---

[41] Google response to November 2023 Consultation, p.3, 33.
[42] [✂]; MSPG response to November 2023 Consultation, p.7. We note that MSPG made a similar point in its response to the May 2024 Consultation, p.7; Online Travel UK response to May 2024 Consultation on Protecting Children from Harms Online, p.7. In its response, Online Travel UK suggested this may be the case in particular where services posed a low risk for breaches of child safety, for example, online travel booking and comparison sites; Reddit response to November 2023 Consultation, p.9; Skyscanner response to November 2023 Illegal Harms Consultation, p.16; Wikimedia Foundation response to November 2023 Illegal Harms Consultation, p.21.
[43] SPRITE+ (JN) response to November 2023 Illegal Harms Consultation, p.6.
[44] BILETA response to November 2023 Consultation, p.5, 9.
[45] Google response to November 2023 Consultation, pp.66-67.
[46] OSA Network response to November 2023 Consultation, Annex C, p.1.
[47] Community Security Trust response to November 2023 Consultation, p.2; Molly Rose Foundation response to November 2023 Consultation, p.9; Name Withheld 1 response to November 2023 Illegal Harms Consultation, p.1; OSA Network response to November 2023 Consultation, p.94; Suzy Lamplugh Trust response to November 2023 Consultation, pp.7-8; Victims' Commissioner for England and Wales response to November 2023 Consultation, p.9.
[48] OSA Network response to November 2023 Consultation, p.99.
[49] OxDEL response to November 2023 Consultation, p.6.
[50] Are, C. response to November 2023 Illegal Harms Consultation, p.6.

number of stakeholders said that the Act and our subsequent approach would lead to censorship and would pose a threat to freedom of expression and privacy in the UK.[51]

1.68 Clean Up the Internet did not agree that our recommendations for the measures were appropriate, or that they would be effective in improving online safety because they could emphasise certain users' rights (such as freedom of expression) without adequately balancing the rights of other users (such as protection from harm). It pointed out that anonymity can be a positive feature for some users but can also negatively affect others.[52]

1.69 The Internet Society expressed concerns about whether the proportionality assessments for encrypted services could lead to arbitrary surveillance and over targeting of users who are not the intended target of the measures.[53]

1.70 The Information Commissioner's Office (ICO) highlighted several areas in the Codes, particularly across moderation measures and reporting and complaints, where it felt that further privacy safeguards were needed, and that more consideration was needed regarding data protection law.[54]

Evidence

1.71 In response to our November 2023 Consultation, several stakeholders raised questions regarding our approach to evidence.[55]

1.72 Some respondents considered that the evidential bar we had set for considering measures was too high, or that we were too focused on evidence from service providers. For example, the Molly Rose Foundation argued that we had adopted a standard of proof more common in criminal law than regulatory regimes ('beyond reasonable doubt').[56] A number of civil society organisations argued that we should apply the 'precautionary principle' and recommend measures where there is a suggested risk of harm (even if evidence of their effectiveness is minimal).[57] 5Rights Foundation also criticised what it saw as our "fixation" on evidence from providers, rather than on evidence of effective harm mitigation.[58] Some respondents disagreed with our use of the term "good practice" in our discussion of evidence of current practices adopted by service providers and shared their belief that

[51] Big Brother Watch response to November 2023 Illegal Harms Consultation, p.1; Bitchute response to November 2023 Illegal Harms Consultation, p.1.
[52] Clean Up the Internet response to the November 2023 Consultation, pp.6-7.
[53] Internet Society response to November 2023 Illegal Harms Consultation, pp.12-13.
[54] ICO response to November 2023 Illegal Harms Consultation, pp.9-21.
[55] Barnardo's response to November 2023 Consultation, p.1, p.9. We note that Barnardo's made a similar point in its response to the May 2024 Consultation, p.3; Community Security Trust response to November 2023 Consultation, p.1; OSA Network response to November 2023 Consultation, pp.3-4. We note that the OSA Network (2) made a similar point in its response to the May 2024 Consultation, pp.31-32; Lucy Faithfull Foundation response to November 2023 Illegal Harms Consultation, p.2. We note that the Lucy Faithfull Foundation made a similar point in its response to the May 2024 Consultation, p.2; Molly Rose Foundation response to November 2023 Consultation, p.5. We note that the Molly Rose Foundation made a similar point in its response to the May 2024 Consultation, p.35; NSPCC response to May 2024 Consultation, pp.23.
[56] Molly Rose Foundation response to November 2023 Consultation, p.5.
[57] Clean Up the Internet response to November 2023 Consultation, p.2; Molly Rose Foundation response to November 2023 Consultation, pp.6-7; We note that the Molly Rose Foundation made a similar point in its response to the May 2024 Consultation, p.9; OSA Network response to November 2023 Consultation, p.34-39.
[58] 5Rights Foundation response to November 2023 Consultation, p.3.

providers are often not meeting the high standard needed when it comes to countering illegal harms.[59]

1.73 Other respondents considered we had not fully taken into account important sources of evidence. We received a range of feedback regarding aligning our approach and evidence with other regimes.

- Several stakeholders felt our approach should align with the Digital Services Act (DSA), or international regulation generally, where possible.[60] One noted how this approach could avoid excessive compliance costs and conflicting standards, and others asked us to avoid conflicting asks.[61] [62] One service provider approved of our ongoing work to collaborate with global regulators.[63] Some stakeholders welcomed alignment with the DSA, but also asked for us to improve "where it has fallen short".[64]
- OnlyFans asked that we consider the definitions already adopted by other legal, industry, and regulatory regimes because most online services operate internationally.[65]
- The Molly Rose Foundation asked us to work with the Competition and Markets Authority (CMA) to mitigate the risk of anti-competitive effects.[66]
- Snap questioned why we had not made greater use of video sharing platform (VSP) regime learnings in our November 2023 Consultation.[67]

1.74 Other stakeholders considered that we would benefit from greater engagement with vulnerable groups and those with lived experiences of illegal and harmful content.[68]

---

[59] Cats Protection response to November 2023 Illegal Harms Consultation, p.9; Community Security Trust response to November 2023 Consultation, p.1; Cyacomb Ltd response to November 2023 Illegal Harms Consultation, p.8; [✂]; OSTIA response to November 2023 Illegal Harms Consultation, p.7; Protection Group International response to November 2023 Illegal Harms Consultation, p.4; Victims' Commissioner for England and Wales response to November 2023 Consultation, p.8.

[60] Family Online Safety Institute (FOSI) response to May 2024 Consultation on Protecting Children from Harms Online, p.4; Meta response to November 2023 Consultation, p.15; Mobile Games Intelligence response to November 2023 Consultation, p.1; TikTok response to May 2024 Consultation, pp.2-3; Ukie response to May 2024 Consultation, p.3; Yoti response to May 2024 Consultation, p.24.

[61] Spotify response to November 2023 Consultation, p.13.

[62] [✂]; U.S. Department of Justice, Office of Privacy and Civil Liberties response to November 2023 Illegal Harms Consultation, pp.2-3.

[63] X response to November 2023 Illegal Harms Consultation, p.1.

[64] MSPG response to November 2023 Consultation, p.5.

[65] OnlyFans response to November 2023 Illegal Harms Consultation, p.4.

[66] Molly Rose Foundation response to November 2023 Consultation, p.6.

[67] Snap response to November 2023 Illegal Harms Consultation, p.4.

[68] Brave Movement response to May 2024 Consultation on Protecting Children from Harms Online, p.1; Children's Commissioner for England response to November 2023 Consultation, p.19; Frida response to November 2023 Consultation, p.7; Glitch response to November 2023 Illegal Harms Consultation, p.4; ICSA Changemakers response to November 2023 Consultation, p.3; NSPCC response to November 2023 Consultation, p.13. We note that the NSPCC made a similar point in its response to the May 2024 Consultation, pp.40-41; NWG Network response to November 2023 Illegal Harms Consultation, p.10; Parenting Focus response to May 2024 Consultation on Protecting Children from Harms Online, p.27; Phoenix 11 response to November 2023 Illegal Harms Consultation, pp.3-4; Samaritans response to November 2023 Consultation, p.1. We note that Samaritans made a similar point in its response to the May 2024 Consultation, p.4.

How we have assessed measures

1.75 When assessing the case for including a measure in Codes, we have considered the following factors:

a) the prevalence and impact of the harm the measure is combatting;
b) the efficacy of the measure in combatting this harm;
c) the direct and indirect costs of the measure;
d) the impact the measure would have on privacy and freedom of expression; and
e) any risks associated with the measure.

1.76 We weigh these factors against one another to assess whether the measure in question is proportionate when seen in the round. As part of this assessment, we consider whether it would be proportionate to apply the measure to all service providers or a subset of service providers. We also consider both the individual and cumulative impact of the measure.

1.77 While we may have evidence of risk existing (or of how it manifests), this does not always translate to evidence of how to proportionately mitigate this risk (as is needed when making recommendations in Codes). For example, we do not always have evidence of which measures are effective or what unintended consequences they may have. The challenges in this area are particularly acute where possible measures have significant human rights impacts (as is the case wherever a measure may involve surveillance, user banning, or the use of proxies for illegal content). They are also acute where possible measures involve the use of proactive technology as the Act sets out extra factors to which we must have regard before we can make recommendations. Unless a particular Codes measure is directly taken from a duty under the Act, we have made recommendations only where we consider we can justify doing so.

1.78 We discuss each component of the impact assessment in more detail below.

Risk of harm

1.79 Our comprehensive assessment of the causes and impacts of illegal harms, as set out in the Register, provides us with a clear understanding of how different kinds of illegal harm manifest online, although we acknowledge there remain some gaps in the evidence base linking specific harms and characteristics. This has helped us to identify measures likely to be effective at protecting users and to target those measures towards services where users face the greatest risks.

1.80 The Register's function is to highlight where we have evidence of how risk manifests on regulated services. Where a recommended measure does not follow directly from the Act, we have set out the risk of harm that we are seeking to address through our recommended measure.

1.81 There are some measures, such as our content moderation measures regarding internal policies and resourcing, which are applicable to all kinds of illegal harm. Some measures target multiple defined kinds of illegal harm (such as user control measures regarding blocking other users and disabling comments).[69] Other measures address a single kind of illegal harm (such as hash-matching to detect known CSAM, fraud reporting channels, and suicide search crisis intervention).[70]

[69] See Volume 2: chapter 12.
[70] See Volume 2: chapters 4,6, and 9.

Benefits and effectiveness

1.82 We have considered how each measure will reduce the risk of harm we have identified and how effectively it will do this. We have considered any evidence of each measure's current use by providers of services of different types and sizes, as well as its technical feasibility. This evidence enables us to assess each measure's proportionality when balanced against its potential costs and any human rights impacts it may have. For measures that recommend proactive technology, we must take into account the degree of accuracy, effectiveness, and lack of bias achieved by the technology.[71]

1.83 While we have sought to quantify impacts where feasible, we have only been able to do this to a limited extent – mainly because of a lack of robust quantitative evidence. It is even more challenging to put certain benefits in monetary terms. For example, it is difficult to quantify the social and psychological impacts of exposure to illegal content and damage to physical and mental health. While we have not generally quantified these benefits in monetary terms, we have placed significant weight on such impacts in our decisions.[72]

1.84 We have used our assessment of the evidence on how (and to what extent) each measure contributes to safer experiences online to design and prioritise measures in line with our objectives (as outlined in Volume 2: chapter 1).

Cost and risks

Costs to providers

1.85 We have considered the impact on providers to ensure that the likely costs associated with a measure are justified. This is partly because imposing costs on providers can have negative impacts or risks for users. For example, if an increased cost burden on providers reduces investment in areas other than user safety or drives some services to stop operating in the UK, this means that users can no longer benefit from such services or new innovations. We are also required under the Act to consider the proportionality of measures having regard to the size and capacity of the provider, and to carry out an impact assessment.[73]

1.86 This does not mean that a measure is necessarily disproportionate because it imposes significant costs on providers or because it creates risk of some services ceasing to operate in the UK. While there may be a loss to users from some services ceasing to operate, this may be in users' overall interest if such services are causing significant harm through illegal content and if providers are not prepared (or cannot afford) to apply a measure to sufficiently address that harm.

1.87 We have considered both direct costs and indirect costs to providers. The direct costs of a measure include both one-off costs and any ongoing costs of implementing it. Where these direct costs are quantified, they rely on salary estimates and other assumptions as detailed in Annex 5 (where we respond to feedback on our approach to quantifying the direct costs

[71] Proactive technology is defined in section 231 of the Act as content identification technology, user profiling technology, or behaviour identification technology.
[72] See for further work regarding value of wellbeing metrics: Ofcom, 2024. Evaluating the Wellbeing Impacts of the Online Safety Act: a Feasibility Study [accessed 4 November 2024].
[73] See sections 10(10) and 27(10) of the Act and section 7 of the 2003 Act (which requires, in particular, that Ofcom include an assessment of the likely impact of implementing the proposal on small businesses and micro businesses).

to providers of implementing our measures). Where we have not quantified costs, we describe their nature.

1.88 Indirect costs to providers may arise, for example, from reduced user engagement where a measure imposes additional frictions to the user journey and reduces revenue.

1.89 Our analysis has focused on costs on a 'per service' basis, rather than on total cost to the sector. We consider that this is a more appropriate way to test the proportionality of the measures. There are a number of reasons for this. Firstly, this approach has allowed us to consider the implications of our measures for services of different sizes and capacities. Given the range of services in scope of the measures, this approach allows us to capture the variety of services that the measures will apply to and to tailor our measures to different types of service. Secondly, there is significant uncertainty about the number and diversity of services in scope of the Act. In this context, it is difficult to meaningfully quantify the aggregate cost to the sector as a whole.

1.90 The broad scope of the regime means the nature of services varies very significantly, as does the access to resources for different kinds of service provider. These factors may influence how different providers will be impacted by our recommended measures. That a particular service provider may incur higher costs than we estimate does not mean that the measure should not be recommended for the purposes of complying with its illegal content safety duties. Service providers have the option to take measures other than those recommended in the Codes but must ensure that these measures are (taken together) sufficient to comply with their illegal content safety duties.

1.91 As detailed in our discussion of the design of measures, we have allowed service providers some flexibility in terms of how they implement our recommendations. In areas where we have been more specific around the details of practical implementation, our assessment and discussion of cost is more detailed.

1.92 In some cases, service providers may already have similar or identical measures in place to those outlined in the Codes. Such providers will be able to comply with the measures for very little additional cost. Our analysis focuses instead on the costs for providers who do not currently have similar or equivalent measures. This is a more rigorous test of whether the measures are proportionate; our measures can only be proportionate if they are proportionate for a provider that is not currently doing them.

1.93 We acknowledge that providers may need to rely on existing staff and technology to implement measures in the short term. Where this diverts resources from more profitable uses, the opportunity cost of implementing measures could be higher than we have assumed. Our approach to quantifying costs implicitly assumes that providers adjust their resources to meet their online safety duties.

Costs to users

1.94 We have also considered indirect costs to users. While the measures are designed to provide benefits to users in the form of protection from illegal harms, some measures may also have detrimental effects. For example, our measures to protect children from grooming may have the indirect cost for adult users of a service by making it harder for them to connect with children online. We have factored in any such detrimental costs and weighed them against the benefits to users when deciding on the overall proportionality of each measure.

Risks

1.95 We have considered potential risks that may arise inadvertently through the implementation of the recommended measures. It is important to consider such risks because, while uncertain, they could increase costs to providers or users if they were to materialise. These risks could also reduce the benefits and effectiveness of the safety measures. For example, frequent crisis prevention warnings might lead users to become desensitised to them – and therefore more likely to ignore them – reducing the effectiveness of the measure. Another example is the risk of CSAM URL lists used for our URL detection measure being obtained by perpetrators and used to help them view such content.

1.96 As far as possible, we have designed our measures to mitigate risks we are able to anticipate. However, it is not always possible to eliminate these risks.

Rights

1.97 In accordance with our obligations under the Human Rights Act 1998, we must consider the impacts that our regulation could have on human rights as set out in the European Convention on Human Rights (ECHR) and ensure that it does not interfere disproportionately with these rights.

Interference with rights or protection of rights

1.98 We recognise that online safety regulation may also help *protect* individuals' human rights. For example, when users feel safe online, they may be more able to exercise their rights to freedom of expression. As set out in 'Introduction, our duties, and navigating the Statement', we start from the position that UK users should be protected from the harms set out in the Act and we take account of the evidence of harm set out in our Register of Risks. An important benefit of protecting users from the harms is that their relevant human rights will be protected. We take this benefit into account as part of the assessment of the benefits of the measure which we discuss above.

1.99 However, protecting victims' and survivors' human rights is implicit in our duty to carry out our functions so as to secure the adequate protection of citizens from harm presented by content on regulated services.[74] We therefore do not think it is necessary to show that a particular harm to a user infringes their human rights in order to show that the user should be protected from that harm.

1.100 Our assessment of human rights in our impact assessment focuses on whether there is reason to think that a measure which would be effective to address the harm amounts to a disproportionate *interference* with human rights. In order to assess this, we need to consider the impacts of each measure on the rights that are being interfered with.

1.101 Victims' and survivors' human rights may also be engaged in relation to measures we do *not* recommend, if the harms to which they are exposed both engage their human rights and are sufficiently serious. However, the Act does not permit us to make recommendations we have not impact assessed. As set out in paragraphs 1.51 to 1.56, we have adopted an iterative approach to our Codes. Delaying the Codes until we have a fuller set of recommendations would deprive users of such protections as we can put in place now.

[74] Section 3(2)(g) of the 2003 Act.

1.102 Accordingly, although we acknowledge some benefits to human rights of our measures in our thinking, the main focus of our analysis for each measure is on whether their benefits overall justify any possible interferences with human rights.

The human rights engaged by our recommendations

1.103 We have considered the potential human rights implications of each measure, in particular the right to freedom of expression (Article 10 ECHR), the right to freedom of association (Article 11), and the right to privacy (Article 8 ECHR).[75] We have sought to ensure that any interference with adults' and children's relevant rights is proportionate to the legitimate objective of the Act of protecting users from harmful content.

1.104 In determining which measures are proportionate to recommend in the Codes, we have carefully considered the right to freedom of expression.[76] However, we note that, as set out in the November 2023 Consultation, a service provider has the right to decide to remove content that is not illegal. This is an exercise of its own right to freedom of expression. We cannot compel a provider to carry content it does not wish to carry, nor can we prevent a provider from taking down content that is not illegal or harmful. We acknowledge the risk that, as a result of our recommendations, a provider may choose to take action against content that is legal in order to ensure that it is compliant with its duties relating to content that is illegal. Where possible, we have sought to mitigate that risk. We have drawn out more clearly in our final Codes where we consider measures act as safeguards for freedom of expression. However, the risk is ultimately one which arises from the scheme of the Act and cannot be mitigated entirely.

1.105 We have also considered impacts on the right to respect for privacy and family life. Along with the right to privacy conferred by Article 8 ECHR, there are various domestic laws relevant to this right. Service providers will need to ensure they comply with UK data protection law, which includes the Data Protection Act 2018, the UK General Data Protection Regulations (UK GDPR) and, where relevant, the Privacy and Electronic Communications (EC Directive) Regulations (PECR).

1.106 Users' rights to data protection are regulated by the ICO. The ICO has a range of data protection compliance guidance which we encourage service providers to consult. In particular, services should familiarise themselves with the ICO's Children's Code, the ICO Commissioner's opinion on age assurance, and the ICO guidance on Online safety and data protection.

1.107 In our impact assessments, we have explained where we consider that data protection laws may be engaged, and we have designed our measures on the basis that those laws will apply. We have drawn out more clearly in our final Codes where we consider measures act as safeguards for privacy.

---

[75] For service providers, the right to peaceful enjoyment of their possessions is also relevant (Article 1 of the First Protocol: "No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law"). However, this in no way impairs the right of the UK to enforce such laws as it deems necessary to control the use of property in accordance with the general interest. We consider the Online Safety Act to be such a law and we consider our impact assessment as a whole to demonstrate that the measures are proportionate.

[76] We have had particular regard to the concerns of the Oxford Disinformation and Extremism Lab, but consider they are best addressed by some of the changes we have made in finalising our Illegal Content Judgements Guidance.

Other important considerations in our impact assessment: evidence

Evidence gathering and engagement

1.108 As an evidence-based regulator, we have used information from a diverse set of sources. We have sought the best available information, irrespective of whether that information has come from industry, civil society, research, or other sources. We are developing measures for a sector with limited previous regulation, and we produced our November 2023 Consultation prior to receiving information-gathering powers. This means that the volume of evidence and independent analysis is limited in some areas.

1.109 We do not agree with the suggestion that we have set the evidential bar too high. Overall, we have applied the threshold required by the Act, and the general principles of public law. Evidence is critical to inform our policies in addition to argument and logic. This ensures that our policies are robust, and that we make proportionate proposals and decisions to protect UK users online. As outlined above, any evidence of harm is taken through our impact assessment framework.

1.110 In setting out our proposals and our decisions we have used a range of evidence, including:

- responses to our July 2022 Call for Evidence;[77]
- responses to our November 2023 Consultation, our May 2024 Consultation, and our August 2024 Illegal Harms Further Consultation on Torture and Animal Cruelty ('August 2024 Further Consultation');
- information gathered through bilateral and other sessions with stakeholders, including engagement with industry groups, civil society groups and groups representing the interests of individuals with lived experience of online illegal harms;
- our own and others' research, including research on evidence around the kinds of and risk of harm online, as well as key areas across Codes and wider Statement documents.
- We have tried, where possible and appropriate, to incorporate learnings from our VSP work and align with international counterparts.

1.111 A number of our measures aim to reduce the regulatory burden on service providers captured by multiple regimes and bring in learnings taken from our other work (for example, regarding our position on terms of service and publicly available statements, reporting and complaints, and user controls). We will continue to work with our international colleagues to stay informed of developments within other regimes and will seek collaboration where possible (including through the Global Online Safety Regulators Network). We will also continue to work with other UK regulators operating in the online and digital space via the Digital Regulation Cooperation Forum (DRCF).

1.112 Online services providers within the scope of the Act (and the technologies they use) are evolving rapidly, and new harms may emerge as a result. There is a need for prompt action to protect people online. Therefore, some of our measures are based on an assessment of more limited or indirect evidence of impact and have a reliance on logic-based rationales. We exercised regulatory judgement in prioritising measures and consider that, on balance, the package will materially improve safety online.

[77] 2022 Ofcom Call for Evidence: First phase of online safety regulation.

Who our measures apply to

November 2023 Illegal Harms Consultation

1.113 Each proposed measure on which we consulted included detail about the services it should apply to. This aligns closely with the requirement for our proposed measures to be proportionate and acknowledges the diversity of services that fall in scope of the measures.

1.114 We proposed different measures for U2U and search services, and in the latter distinguished between general and vertical search services.[78] Beyond that, we proposed to break down services in scope of the Act into a number of broad types:

a) We defined services which were medium or high risk for a particular harm as 'single risk' services;
b) We defined services that were medium or high risk for two or more kinds of illegal harm as 'multi-risk' services. We considered that it was important to differentiate between single risk and multi-risk services. Where service providers only identify a risk of a single kind of illegal harm the expected benefits of applying our measures that address all harms would be lower compared to services with risks of multiple kinds of illegal harm.
c) We proposed services with an average user base greater than seven million monthly UK users. We proposed to define UK users in line with the Act for the purposes of determining whether a service is 'large'. The Act specifies that it does not matter whether a person is registered to use a service. We also said that the average monthly number of UK users should be calculated over 12 months. Our approach of taking user base as a proxy for the size of a service was similar to that adopted by the European Union in the DSA.

1.115 Dividing up services in this way allowed us to take a proportionate and risk-based approach. All else being equal, our draft Codes imposed more onerous expectations on services which were larger or higher risk than on services which were smaller and lower risk.

Feedback

1.116 Some stakeholders supported our consideration of size, functionality, and risk when drafting the measures.[79]

1.117 Several stakeholders agreed with our threshold and reasoning for multi-risk, including civil society organisations, public organisations, and some service providers.[80]

---

[78] See Overview of regulated services chapter for more details.

[79] Association of Police and Crime Commissioners response to November 2023 Consultation, p.4; Name Withheld 5 response to November 2023 Illegal Harms Consultation, pp.4-5; 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.3; Match Group response to November 2023 Consultation, p.7; MSPG response to November 2023 Consultation, p.5; Proton response to November 2023 Illegal Harms Consultation, p.4; Trustpilot response to November 2023 Illegal Harms Consultation, p.12.

[80] ACT | The App Association response to November 2023 Illegal Harms Consultation, p.9; Are, C. response November 2023 Consultation, p.6; Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) response to November 2023 Illegal Harms Consultation, p.7; Cifas response to November 2023 Consultation, p.8; [✂]; Evri response to November 2023 Illegal Harms Consultation, p.4; INVIVIA, Inc response

1.118 Furthermore, many stakeholders agreed that the most onerous measures should apply to services classified as large and/or multi-risk (even if they did not agree with all aspects of the definition).[81]

1.119 Several stakeholders agreed with our definition of a 'large' service as being one with more than seven million monthly UK users, including some that appreciated the broad alignment with the DSA.[82]

---

to November 2023 Illegal Harms Consultation 2023, p.10; Local Government Association response to November 2023 Illegal Harms Consultation, p.7; Marie Collins Foundation response to November 2023 Illegal Harms Consultation, p.9; Match Group response to November 2023 Consultation, p.8; Mencap response to November 2023 Illegal Harms Consultation, p.8; OnlyFans response to November 2023 Illegal Harms Consultation, p.4; National Trading Standards eCrime team response to November 2023 Consultation, p.7; Nexus response to November 2023 Illegal Harms Consultation, p.9; NSPCC response to November 2023 Consultation, p.17; Royal Society for the Prevention of Cruelty to Animals (RSPCA) response to November 2023 Illegal Harms Consultation, p.4; Scottish Government response to November 2023 Illegal Harms Consultation, p.5; Scottish Society for Prevention of Cruelty to Animals (SSPCA) response to November 2023 Illegal Harms Consultation, p.9; Segregated Payments Limited response to November 2023 Consultation, p.7; Stop Scams UK response to November 2023 Consultation, p.10; WeProtect Global Alliance response to November 2023 Consultation, p.11.

[81] ACT | The App Association response to November 2023 Consultation, p.8; Are, C. response to November 2023 Consultation, p.6; CarefulAI response to November 2023 Illegal Harms Consultation, p.5; CCDH response to November 2023 Consultation, p.10 (we note that CCDH also disagreed with our definition of and threshold for 'multi-risk'); Centre for Competition Policy response to November 2023 Consultation, p.17; CELE response to November 2023 Consultation, p.7; Dwyer, D. response to November 2023 Consultation, p.4; Evri response to November 2023 Consultation, p.4; Greater Manchester Combined Authority response to November 2023 Illegal Harms Consultation, p.8; Lloyds Banking Group PLC response to November 2023 Illegal Harms Consultation, p.8; Logically response to November 2023 Consultation, p. 16; Marie Collins Foundation response to November 2023 Consultation, p.8; Match Group response to November 2023 Consultation, pp.7-8; Mencap response to November 2023 Consultation, p.7; Mental Health Foundation response to November 2023 Illegal Harms Consultation, p.1; Microsoft response to November 2023 Illegal Harms Consultation, p.7 (we note that Microsoft also disagreed with our definition of and threshold for 'multi-risk'); Name Withheld 2 response to November 2023 Illegal Harms Consultation, p.6; OnlyFans response to November 2023 Consultation, p.5; National Trading Standards eCrime Team response to November 2023 Consultation, p.6; Nexus response to the November 2023 Consultation, p.7; RSPCA response to November 2023 Consultation, p.4; Safe Space One response to November 2023 Illegal Harms Consultation, p.8; South East Fermanagh Foundation response to November 2023 Consultation, p.6; Segregated Payments Limited response to November 2023 Consultation, p.6; Stop Scams UK response to November 2023 Consultation, p.9; Ukie response to November 2023 Consultation, p.12 (we note that Ukie disagreed with how services were designated as medium, high or multi-risk; see Ukie response to November 2023 Consultation, pp. 6-8, 12, 14).

[82] ACT | The App Association response to November 2023 Consultation, pp.8-9; Alliance to Counter Crime response to November 2023 Consultation, p.5; Are, C. response to November 2023 Consultation, p.6; BILETA response to November 2023 Consultation, p.7; Bolton, C. response to November 2023 Illegal Harms Consultation, p.4; Centre for Competition Policy response to November 2023, p.18; CELE response to November 2023 Consultation, p.7; [✂]; Name Withheld 5 response to November 2023 Consultation, p.5; Dwyer, D. response to November 2023 Consultation, p.4; Evri response to November 2023 Consultation, p.4; Global Partners Digital response to November 2023 Consultation, p.12; Local Government Association response to November 2023 Consultation, p.6; Marie Collins Foundation response to November 2023 Consultation, p.8; Match Group response to November 2023 Consultation, p.8; Mencap response to November 2023 Consultation, p.7; National Trading Standards eCrime Team response to November 2023 Consultation, p.6; Nexus response to November 2023 Consultation, p.8; RSPCA response to November 2023 Consultation, p.4; Safe Space One response to November 2023 Consultation, p.8; Segregated Payments Limited response to November 2023 Consultation, p.6; Scottish Government response to November 2023 Consultation, p.5; SSPCA response to November 2023 Consultation, p.8; Trust Alliance Group response to November 2023 Illegal Harms Consultation, p.7; Stop Scams UK response to November 2023 Consultation, p.9; WeProtect Global Alliance response to November 2023 Consultation, p.10.

1.120 However, several respondents disagreed with aspects of our approach.

Multi-risk services

1.121 A number of respondents disagreed with our approach to multi-risk services. One stakeholder said our approach provided an incentive for providers to downplay risks to evade being classed as multi-risk.[83] Some stakeholders considered that many or all of our measures should be extended to all services.[84] Some civil society groups argued that child safety measures should apply to all U2U services.[85] The Welsh Government said that services popular among children should be considered high-risk and thus should apply the most onerous measures, and that we should ensure minority groups such as Welsh speakers did not receive less protection due to our definitions of risky or large services.[86] In contrast, some providers felt that the measures we proposed for multi-risk services could be too onerous for small services.[87]

1.122 Some respondents also said we had assumed, without evidence, that single-risk services would be less harmful, and argued that providers of small single-risk services should have to apply multi-risk measures.[88] One stakeholder said flexibility should be given for more onerous measures to apply to services who present high-volume risk of a single form of illegal content.[89] Respondents gave examples of services that are geared towards the sharing of a specific type of content, such as 'revenge porn' collector sites or suicide forums, which they said could be extremely harmful.[90] The OSA Network argued that it did not make sense to recommend that providers of single-risk services should be aware of their risks without recommending that they mitigate them.[91] Some respondents said we

[83] Institute for Strategic Dialogue response to November 2023 Consultation, p.8.
[84] Board of Deputies of British Jews response to November 2023 Illegal Harms Consultation, p.3; International Justice Mission response to November 2023 Illegal Harms Consultation, p.9; Protection Group International response to November 2023 Consultation, pp.4-5, 13; Yoti response to November 2023 Consultation, pp.14-15, 24.
[85] C3P response to May 2024 Consultation on Protecting Children from Harms Online, p.17; Children's Commissioner for England response to November 2023 Consultation, p.21. We note that the Children's Commissioner made a similar point in response to the May 2024 Consultation, p.53.
[86] Welsh Government response to November 2023 Illegal Harms Consultation, p.3.
[87] BitChute response to November 2023 Consultation, p.2; Mega response to November 2023 Illegal Harms Consultation, p.4.
[88] 5Rights Foundation response to November 2023 Consultation, p.20; Barnardo's response to November 2023 Consultation, p.13; Bereaved Families for Online Safety response to November 2023 Consultation, p.2; C3P response to November 2023 Consultation, p.5; We note that C3P made a similar point in its response to the May 2024 Consultation, pp. 17-19; CCDH response to November 2023 Consultation, p.10; Cyber Helpline response to November 2023 Consultation, p. 10; IWF response to November 2023 Consultation, pp.21-22; OSA Network response to November 2023 Consultation, pp.77-80; We note that the OSA Network (2) made a similar point in its response to the May 2024 Consultation, pp.54-55, 63; Samaritans response to November 2023 Consultation, p.3; Sanders, T. response to November 2023 Illegal Harms Consultation, p.7; Suzy Lamplugh Trust response to November 2023 Consultation, p.8.
[89] Lloyds Banking Group PLC response to November 2023 Consultation, p.8;
[90] 5Rights Foundation response to November 2023 Consultation, p.19; Alliance to Counter Crime Online response to November 2023 Consultation, p.5; C3P response to May 2024 Consultation, p.10; EVAW response to November 2023 Consultation, pp.14-15; Institute for Strategic Dialogue response to November 2023 Consultation, p.8; Molly Rose Foundation response to November 2023 Consultation, pp.30-31; OSA Network response to November 2023 Consultation, p.80; Refuge response to November 2023 Consultation, pp.9-10.
[91] OSA Network response to November 2023 Consultation, pp.77-80.

were incorrect in stating that providers of single-risk services were likely to better understand the harm posed on their service.[92]

1.123 We also received suggestions that we should raise the threshold from two kinds of illegal harm for multi-risk services (namely, that we should define the threshold so that services needed to pose a high risk of more than two harms before they were in scope of the measures applicable to 'multi-risk' services). Some service providers and representative groups considered that we lacked a clear rationale for proposing this threshold.[93] Others argued that the threshold we set was too low, and several further suggested that service providers in scope of the multi-risk measures should be those at risk of a higher number of harms.[94] Some respondents said that our definition may capture most services and thus lacked nuance.[95] Others argued that we should establish further thresholds to differentiate between services at risk of two kinds of illegal harms and services at risk of ten or fifteen kinds.[96] Some respondents asked for a distinction between services that are found to be "medium risk" and "high risk", with some wanting more onerous measures applicable to the latter group.[97] Stakeholders also raised concern about overlaps in some kinds of illegal harm, and the impact of this on the definition of multi-risk services.[98] Meta argued that we should be more consistent across our documents as to whether the CSEA offences should be considered as distinct kinds of illegal harms, which affects whether a service is defined as multi-risk.[99]

---

[92] C3P response to May 2024 Consultation, pp.10-11; IWF response to November 2023 Consultation, p.22.

[93] Microsoft response to November 2023 Consultation, p.9; Trustpilot response to November 2023 Consultation, pp.18-19, Ukie response to November 2023 Consultation, p.14.

[94] [✂] Dwyer, D. response to November 2023 Consultation, pp.1-2; Microsoft response to November 2023 Consultation, p.9; MSPG response to November 2023 Consultation, p.5; Online Dating and Discovery Association response to November 2023 Illegal Harms Consultation, p.1; Pinterest response to November 2023 Consultation, p.5.We note Pinterest made a similar point in response to May 2024 Consultation, pp.10; Proton response to November 2023 Consultation, p.5; Reddit response to November 2023 Consultation, pp.5, 7, 25; Roblox response to November 2023 Consultation, p.18; Skyscanner response to November 2023 Consultation, pp.14-15; Spotify response to November 2023 Illegal Harms Consultation, p.5; techUK response to November 2023 Consultation, p.21; Trustpilot response to November 2023 Consultation, pp.19-20; Twelve APP response to May 2024 Consultation on Protecting Children from Harms Online, p.13; Ukie response to May 2024 Consultation, p.35.

[95] Center for Data Innovation response to November 2023 Consultation, p.9; Mega response to November 2023 Illegal Harms Consultation, pp.4-5; Microsoft response to November 2023 Consultation, p.9; Name Withheld 2 response to November 2023, p.6; Pinterest response to November 2023 Consultation, p.5.

[96] [✂] Name Withheld 5 response to November 2023 Consultation, pp.7; LinkedIn response to November 2023 Consultation, p.8; Meta response to November 2023 Consultation, pp.19-20; Microsoft response to November 2023 Consultation, p.9; Roblox response to November 2023 Consultation, p.18; techUK response to November 2023 Consultation, p.21.

[97] Airbnb response to November 2023 Consultation, p.11; Booking.com response to November 2023 Consultation, p.7; Google response to November 2023 Consultation, p.27. We note Google made a similar point in response to May 2024 Consultation on Protecting Children from Harms Online, p.22;

[98] [✂] techUK response to November 2023 Consultation, p.21.

[99] Meta response to November 2023 Consultation, pp.4-5, pp19-20.

Size of service

Small services

1.124 Some stakeholders were concerned about the overall burden of measures (and the Act more generally) on smaller services.[100] Some noted that this could include smaller providers offering services on a non-commercial basis, including those provided by individuals in their spare time.[101]

1.125 Other stakeholders expressed concerns that if some small service providers receive less scrutiny (such as those without a particular risk or with a single risk), this could create perverse outcomes, or they could become places to which illegal content migrates.[102]

Large services

1.126 In response to our definition of large services, we received challenges to our perceived focus on size (as opposed to risk). These included arguments that smaller services may also face a significant risk of illegal content, or that large services may not be inherently risky.[103] Some service providers opposed the idea that size alone should influence the degree to which a service is regulated.[104] Some stakeholders argued that the definition of large

---

[100] BILETA response to November 2023 Consultation, p.19; Bolton, C. response to November 2023 Consultation, pp.1, 11; Digital Trust and Safety Partnership (DTSP) response to November 2023 Illegal Harms Consultation, p.5; Dwyer, D. response to November 2023 Consultation, pp.2-3, 11-12; Element response to November 2023 Illegal Harms Consultation, p.6; Federation of Small Businesses response to November 2023 Consultation, p.3; Name Withheld 3 response to November 2023 Consultation, pp.3, 9, 12, 20; MSPG response to November 2023 Consultation, pp.9-10; Ukie response to November 2023 Consultation, pp.14-15.

[101] Bolton, C response to November 2023 Consultation, pp.1, 11; Global Network Initiative response to November 2023 Consultation, p.8; Name Withheld 3 response to November 2023 Consultation, pp.3, 9, 12, 20.

[102] Board of Deputies of British Jews response to November 2023 Consultation, p.3; Cyber Helpline response to November 2023 Consultation, p.3; Greater Manchester Combined Authority response to November 2023 Consultation, p.8; The Independent Reviewer of Terrorism Legislation response to November 2023 Illegal Harms Consultation, p.6; IWF response to November 2023 Consultation, p.20; LinkedIn response to November 2023 Consultation, pp.18-19; NSPCC response to November 2023 Consultation, pp.15-16; OxDEL response to November 2023 Consultation, p.6; Refuge response to November 2023 Consultation, p.9; Samaritans response to November 2023 Consultation, pp.3-4; South East Fermanagh Foundation response to November 2023 Consultation, p.7; Snap response to November 2023 Consultation, p.23; Yoti response to November 2023 Consultation, p.25.

[103] Association of Police and Crime Commissioners response to November 2023 Consultation, pp.3-4; C3P response to May 2024 Consultation, p.17; CCDH response to November 2023 Consultation, p.9. We note that the CCDH made a similar point in its response to the May 2024 Consultation, p.7; Google response to November 2023 Consultation, p.15; Institute of Strategic Dialogue response to November 2023 Consultation, p.8; Internet Matters response to November 2023 Illegal Harms Consultation, p.11; IWF response to November 2023 Consultation, pp.20-21. We note that the IWF made a similar point in its response to the May 2024 Consultation, p.5; Molly Rose Foundation response to November 2023 Consultation, pp.30-31; [✂]; NSPCC response to November 2023 Consultation, p.15. We note that the NSPCC made a similar point in its response to the May 2024 Consultation, pp.42-43; OSA Network response to November 2023 Consultation, pp.71-82. We note that OSA Network made a similar point in its response to the May 2024 Consultation, p.55; OxDEL response to November 2023 Consultation, pp.6-7; Pinterest response to May 2024 Consultation, p.10; Roblox response to May 2024 Consultation, p.18-19; Snap response to May 2024 Consultation on Protecting Children from Harms Online, p.13; South West Grid for Learning response to November 2023 Illegal Harms Consultation, pp. 12-13; Trust Alliance Group response to November 2023 Consultation, p.7; Ukie response to May 2024 Consultation, pp.33-34; UKSIC response to May 2024 Consultation, p.30; Victims' Commissioner for England and Wales response to November 2023 Consultation, p.9.

[104] Airbnb response to November 2023 Consultation, p.12; [✂]; Center for Data Innovation response to November 2023, p.7; Meta response to November 2023 Consultation, p.19; Microsoft response to November 2023 Consultation, p.8; Spotify response to November 2023 Illegal Harms Consultation, p.12.

services or other thresholds for applying more onerous measures could capture public interest or not-for-profit services, which it said were usually lower risk.[105] One respondent argued that our approach of putting additional measures on large services would allow smaller services to gain a competitive advantage due to lower safety costs.[106]

1.127 Regarding the use of user base to determine service size, some stakeholders argued that the threshold should be lower than seven million monthly UK users, while some service providers thought it should be higher.[107] Some suggested tying the definition of 'large' to revenue, employee numbers, or other factors either than or along with user base size.[108] Skyscanner disagreed with the similarity to the DSA approach, noting the difference in size. between the EU market and the UK.[109]

1.128 Several respondents asked for clarification of the definition of 'user'.[110] Some said that the definition should align with that used at EU level by the DSA, while others asked us not to align with the DSA definition of 'user'.[111] Some service providers argued that the Act's definition of 'user' made measurement difficult (or even impossible).[112] Some said that service providers should be given more flexibility over how to calculate user numbers, or advice on how to go about measuring.[113] [114] Google and Trustpilot argued that the calculation of user numbers should be over six months rather than 12 months, noting that

---

[105] Global Partners Digital response to November 2023 Consultation, p.12; H, Julia response to November 2023 Illegal Harms Consultation, p.1.

[106] Snap response to November 2023 Consultation, p.4.

[107] 9000 Lives response to May 2024 Consultation on Protecting Children from Harms Online, p.1; BT Group response to November 2023 Illegal Harms Consultation, p.2; CARE response to November 2023 Consultation, pp.6-7; CCDH response to November 2023 Consultation, pp.9-10; Google response to November 2023, p.28. We note that Google made a similar point in its response to the May 2024 Consultation, p.22; Institute of Strategic Dialogue response to November 2023 Consultation, p.8; International Justice Mission response to November 2023 Consultation, p.9; IWF response to November 2023 Consultation, p.21; Lloyds Banking Group PLC response to November 2023 Consultation, p.8; Reddit response to November 2023 Consultation, pp.5-7; Refuge response to November 2023 Consultation, p.10; Trustpilot response to November 2023 Consultation, pp.14-15; UK Finance response to November 2023 Consultation, p.13; Yoti response to November 2023 Consultation, p.15.

[108] Cifas response to November 2023 Consultation, p.6.; Digital Trust and Safety Partnership response to November 2023 Consultation, p.6; Name Withheld 2 response to November 2023 Consultation, p.6; Reddit response to November 2023 Consultation, p.6; Which? response to November 2023 Illegal Harms Consultation, pp.3-4.

[109] Skyscanner response to November 2023 Consultation, p.13.

[110] Name Withheld 5 response to November 2023 Consultation, pp.5-6; Google response to November 2023 Consultation, p.28. We note that Google made a similar point in its response to the May 2024 Consultation, p.22; Microsoft response to November 2023 Consultation, p.8; techUK response to November 2023 Consultation, p.19. We note that techUK made a similar point in its response to the May 2024 Consultation, p.11; Tremau response to November 2023 Illegal Harms Consultation, pp.2-7; Trustpilot response to November 2023 Consultation, pp.13-14.; Ukie response to May 2024 Consultation, p.33; X response to May 2024 Consultation on Protecting Children from Harms Online, pp.1-2.

[111] Meta response to November 2023 Consultation, p.19; Microsoft response to November 2023 Consultation, p.8; OnlyFans response to November 2023 Consultation, p.4; U.S. Department of Justice, Office of Privacy and Civil Liberties response to November 2023 Illegal Harms Consultation, p.1; Ukie response to November 2023 Consultation, p.12.

[112] Center for Data Innovation response to November 2023 Consultation, pp.7-8; Google response to November 2023 Consultation, p.28; Name Withheld 2 response to November 2023 Consultation, p.6; Proton response to November 2023 Consultation, p.4; [✂[]✂]; Wikimedia Foundation response to November 2023 Consultation, pp.19-20.

[113] Google response to November 2023 Consultation, p.28;

[114] [✂[ ]✂]; Center for Data Innovation response to November 2023 Consultation, pp.7-8.

this aligned with DSA methodology.[115] Some stakeholders expressed concern that service providers might artificially split services to avoid reaching the threshold of seven million monthly UK users.[116]

Service type and functionality

1.129 We received a number of responses concerning the proportionality of our proposed measures for different types of services and functionalities.[117]

1.130 Some stakeholders raised concern that measures showed a lack of consideration for non-traditional moderation systems or 'decentralised' services, and said that applying them would undermine fundamental elements of such services.[118] We also received questions and criticism regarding how our measures were effective for services that use virtual reality (VR) or augmented reality (AR).[119] Some stakeholders also explained that our measures may pose a challenge for end-to-end encrypted services to implement. We received these challenges to both our overall approach and to individual measures.

Downstream search

1.131 Several stakeholders queried whether the duties imposed on search services by the Act apply to a downstream entity on the basis that they may not be the 'provider' of the service as defined by the Act.[120] Responses extended to concerns about the applicability or technical feasibility of our measures and about the appropriateness of our risk profiles, considering the unique manner in which downstream general search services are operated compared to other general search services.

How we have applied measures

1.132 We have applied some measures to all service providers. Most of these recommended measures relate directly to explicit duties in the Act (such as our terms of service measures).

1.133 Where the Act establishes a proportionality test in relation to the services to which a measure should apply, we have not taken a one-size-fits-all approach. We have considered the nature and level of risk of illegal content represented by a service, the harm this illegal content can do to people, the service's functionalities and size, and the capacity of the provider.

---

[115] Google response to November 2023 Consultation, pp.29-30; Trustpilot response to November 2023 Consultation, p.15.
[116] SPRITE+ (Manchester University) response to November 2023 Consultation, pp.7-8; UK Finance response to November 2023 Consultation, p.11; Which? response to November 2023 Consultation, p.4.
[117] Mega response to May 2024 Protecting Children from Harms Online Consultation, p.9; REPHRAIN response to May 2024 Consultation, p.23.
[118] Element response to November 2023 Illegal Harms Consultation, p.6; Wikimedia Foundation response to November 2023 Consultation, p.5.
[119] Barnardo's response to November 2023 Consultation, p.10; OSA Network response to November 2023 Consultation, p.98; REPHRAIN response to May 2024 Consultation, p.23; UKIE response to May 2024 Consultation, p.36.
[120] [✂] [✂]; Ofcom/Ecosia meeting, 30 April 2024; techUK response to November 2023 Consultation, p.22; [✂].

1.134 Therefore, a crucial part of our decision-making concerns which kinds of services each measure should apply to. The measures we are recommending may have different impacts on services of different kinds and sizes and their providers.

1.135 The decisions we explain below affect many of our measures. In the rest of this Statement, we do not repeat these explanations and decisions unless they make a difference to our analysis of the proportionality of the measure. Stakeholders should therefore assume that these points apply to our individual Code measures, where relevant.

Applying more measures to risky services

1.136 A key driver for which services we apply measures to has been the nature and level of risk of illegal harm represented by a service. We have applied more measures to providers of risky services. The benefits to users will be greater, and this is consistent with ensuring proportionality.

1.137 We rely on providers' own assessment of their risk. While in theory this could give them an incentive to understate their risk, they have a duty to undertake a 'suitable and sufficient' risk assessment and we have given guidance on what this means. We are responsible for ensuring providers meet their duty to undertake such a suitable and sufficient risk assessment. If a provider does not do this and understates its risks, we can take enforcement action against the provider for breach of its risk assessment duty. We can also require the provider to take steps to mitigate risks we identify.[121]

1.138 Some measures are targeted at addressing the risk of specific kinds of illegal harm, such as those relating to CSEA, fraud, and foreign interference offences. Whether these measures are proportionate can depend on how risky a service is for the relevant kinds of harm. Typically, our harms-specific recommendations only apply to services whose providers have identified a medium or high risk of relevant kind of harms in their latest illegal content risk assessment. Where proportionate, we have applied these measures broadly. For example, the grooming measures apply in relation to all services with a high risk for grooming, regardless of size.

Multi-risk services

1.139 As well as measures aimed at specific kinds of illegal harm, we also recommend cross-cutting measures aimed at illegal harms generally. Examples of such measures are those on governance and content moderation.

1.140 Most of these measures apply to providers of services that are multi-risk as they face significant general risks and are likely to have large amounts of illegal content to consider. Some of these measures are also about enabling providers to have a good understanding of their risks. This is more important if the provider is at risk for more than one kind of illegal harm, as the different risks are less likely they are to be well understood across the organisation.

1.141 We do not agree with stakeholders that the bar for multi-risk services should be raised from two or more kinds of illegal harm to a higher number. We maintain our position from the

[121] We have amended the drafting of the Codes so that it is clear that measures applicable when the provider is at medium or high risk for kinds of harms will apply both: (a) when the service has identified those risks in a risk assessment; and (b) when, following enforcement against the provider for failure to carry out a suitable and sufficient risk assessment, Ofcom has required the provider to comply with the safety duties as if it had identified those risks.

November 2023 Consultation that the measures offer material benefits when applied to providers of services with medium or high risks of two or more kinds of illegal harms as there are significant risks of users encountering illegal content. We therefore remain of the view that this threshold helps reduce such risks (subject to the proportionality assessment of each measure).[122]

1.142 In principle, we do not consider that there is a proportionality concern if the same list of measures applies to service providers with two kinds of harm as those with many kinds of harm. Most of the multi-risk measures are flexible and to some extent costs increase with the number of harms (and hence with benefits).[123] In practice, we do not expect service providers with different numbers of harms to apply most of the measures in the same way or incur the same costs. For example, the staff compliance training provided by a service with 10 kinds of harms is likely to be longer compared to a service with two kinds of harms because it will need to cover a larger number of risks and the processes involved in identifying and managing them.

1.143 We have revisited the groupings of some of the kinds of illegal harm, and revised and clarified how this works with our definition of multi-risk services.[124] As set out in the Register of Risks, we have mostly grouped harms that are legally overlapping. However, where the harms have very different impacts and users affected may have very different needs, we consider that they should be risk assessed separately and considered separately for the purposes of the definition of multi-risk. We have not grouped harms which occur in overlapping ways. While we accept that a provider whose service focuses, for example, on image-sharing between adults might be at risk of CSEA, intimate image abuse, and extreme pornography, we consider that these are three separate harms with different impacts on users and different potential mitigations. Therefore, it is in our view right that such a provider may be considered multi-risk.

1.144 We have also provided further clarity in the Risk Assessment Guidance about the harms that services must consider in their risk assessments, how to assess them, and how the Codes map onto specific harms where relevant.[125]

1.145 In the November 2023 Consultation, we outlined that we did not consider it proportionate to propose measures targeting all harms when a service has identified a medium or high

---

[122] See details for each measure in the Volume 1: Chapter 5, Volume 2: Chapter: 2, Volume 2: Chapter 3, Volume 2: Chapter 6.

[123] See details for each measure in the Volume 1: Chapter 5 and Volume 2: Chapter: 2

[124] In recognition of their differences, we have separated unlawful immigration from human trafficking in our groupings of harm. We have also made sure the harms groupings only include priority offences, consistent with Parliament's decision that they should be a priority. Consequently, we have taken encouragement of self-harm out of the definition of multi-risk. (This type of content is however primary priority content that is harmful to children, to which our Children's Safety Codes will apply). Finally, one of the priority offences listed in the Act has been repealed since the Act was passed so we have removed it. This is s.50A of the Criminal Law (Consolidation) (Scotland) Act 1995 (racially-aggravated harassment). We do not consider it makes a practical difference to our proposals as the English/Welsh equivalent offence under the Crime and Disorder Act 1998 remains a priority offence and in this context applies in relation to the whole of the UK.

[125] Specifically, providers of U2U services are expected to conduct additional risk level assessments in relation to CSEA. As well as assessing the risk of CSEA overall, they also need to assess for smaller categories of offences within CSEA, namely for CSAM imagery, CSAM URLs, and grooming. This is because these different types of offences are associated with specific risk factors and because we have measures in the Codes where the application of the measure depends on whether the service has a specific kind of CSEA risk. For the purposes of whether they are multi-risk, these components of CSEA all jointly count as only one kind of harm.

risk for a single kind of illegal harm. This is because of the lower extent of harm and lower benefits of these measures (in terms of improving understanding of risks and having a consistent approach to moderate them) than if there were multiple areas of risk. Based on the evidence currently available to us, we remain of the view that the measures are unlikely to have material benefits for smaller low-risk services. However, we acknowledge that at least some of the measures may potentially have material benefits for some single-risk services. In Spring 2025, we intend to consult further on the case for applying some or all of the measures currently recommended only to multi-risk services to some or all single-risk services.

Small and micro businesses

1.146 When considering the proportionality of a measure, we have paid particular attention to potential impacts on small and micro businesses.[126] Even measures which might be considered to have only low to moderate costs may have a significant cost impact on micro businesses. Services provided by small and micro businesses are unlikely to be classed as 'large' services as a business would be likely to need more than 50 employees to provide a service to seven million monthly UK users.

1.147 In many cases, smaller services may pose a lower risk because they reach fewer users. If a service provided by a small or micro business has low risks for all kinds of illegal harm, we will apply few measures beyond those directly required by the Act.

1.148 On the other hand, some services provided by small or micro businesses can present significant risks of illegal harms. In this case, it may be proportionate to apply more measures to protect users. This is despite the fact there may be a significant negative financial impact on the provider. We recommend costly measures for such services where there is clear risk of harm and where there are good reasons for expecting such measures to make a material difference in dealing with this risk. For example, we apply the CSAM hash matching measure to all file-storage and file-sharing services (which pose a particular risk for CSAM) that are high risk for CSAM, regardless of their size.

1.149 We have considered the potential impact of our measures on competition between services when deciding on the proportionality of our measures. We recognise that providers of smaller services may have an advantage if measures do not apply to them, which do apply to providers of larger services. We are less concerned about this – partly because if these services grow and become large services, they will also be subject to the same measures.

1.150 We are more concerned that our measures may hinder providers of smaller services. Our decisions could have a detrimental impact on competition if, for example, some smaller services were not set up because of the online safety measures, or some services did not expand as they might otherwise have done. This is relevant because competition is good for users in providing more choice, driving innovation, and putting downward pressure on prices. We consider any detrimental impact on competition will be small, because some measures are only recommended for providers of large services. If there were an impact on competition because of the effect of our measures on small services that are risky, we consider that to be justified in light of the wider safety ambitions of the Act.

[126] We define such businesses based on the number of full-time equivalent employees, which we understand to be commonly used parameters for defining these businesses across UK Government departments. We define small businesses as those that employ between 10 and 49 full-time equivalent employees, and micro businesses as those that employ between one and nine full-time equivalent employees.

1.151 Our impact assessment for individual measures takes into consideration the potential for user displacement where relevant (see Volume 2: chapter 11). If migration of perpetrators and illegal content to smaller services occurs, the providers of those services will be assessed as high risk in future risk assessments and the relevant measures will apply to them.[127]

1.152 Our assessment singles out small and micro businesses because we have a particular duty to consider them.[128] We recognise the Act also applies to non-commercial entities. Where such entities are small, we consider that they may face similar impacts to those faced by small or micro businesses.

1.153 As well as considering the case for each measure individually, we discuss the combined impact of the set of measures we have recommended for small and micro businesses in Volume 2: chapter 13: 'Combined impact assessment'.

Applying more measures to larger services

1.154 Our approach aims to reduce the risk of harm. For larger services the total risk of harm is likely to be higher even if the likelihood of being exposed to illegal content is low, because such services reach many people. We therefore recommend some measures for providers of large services only. For providers of large services with relevant risks, this includes measures relating to additional user controls, a dedicated reporting channel for trusted flaggers for fraud, and having an internal monitoring and assurance function.

1.155 The costs of such measures may be significant, and those costs could have a material effect on the ability of some smaller service providers to continue to operate.[129] There is often significant uncertainty in our assessment of the benefits and costs of imposing a measure. We aim to reduce the risk of imposing costs on businesses where the size of the potential benefits are uncertain. By not recommending some measures for smaller services, we reduce the risk that such services may be withdrawn for UK users. However, as we explain above, we impose onerous measures on smaller services where they pose a significant risk.

1.156 We also apply some measures to providers of large services even if they have assessed themselves as low risk for all kinds of illegal harm. This applies to, for example, some governance and moderation measures. We consider the recommended measures will have benefits for all large services. There are several reasons for this.

- First, the greater importance of correctly identifying risks for large services compared to smaller services. For example, a failure in oversight of risk management by the provider of a large service would affect a large number of users and so could have a significant adverse impact.[130]

[127] As part of the Act Ofcom requires service providers to conduct risk assessments on at least an annual basis.
[128] See s.7 of the 2003 Act. One response criticised our references to 'businesses', because many services in scope of the measures are operated by private individuals on a non-commercial basis. See Name Withheld 2 response to November 2023 Consultation, p.17.
[129] This is particularly likely to be the case when the measures require large one-off costs that do not vary in magnitude with the size of the service.
[130] If a service has weak online safety governance, this may affect its ability to properly identify risks because it will not have accurate evidence from across the organisation to feed into its risk assessment. As set out in Volume 1: Chapter 5], the measures have material benefits in terms of improving the ability of a large service to identify and mitigate risks. This may be particularly important for providers of large services as they may be more complex organisations.

- The content moderation and search moderation measures are also important because large services may have a substantial volume of content to review and a large number of moderators.[131] Also, if a large service were to incorrectly assess itself as low risk, the recommended measures will contribute to reducing the risks on the service.
- The recommended measures will also help services to identify emerging risks, as risk levels are dynamic and may change quickly. While we expect service providers to identify and mitigate new risks when they update their risk assessments, we do not consider that this addresses emerging risks that can harm many users in a short space of time.

1.157 Applying some measures only to large services is one way in which we have considered the capacity of providers when considering the proportionality of measures.

1.158 We accept that providers of not-for-profit services may have fewer resources than commercial services. However, we maintain that all service providers need to consider the actual level of risk of their service, regardless of type. Even providers that are well-intentioned can carry risk of illegal content. Providers cannot decline to address the risks of illegal harm merely because there are costs associated with doing so. In recognition that the resources available to providers vary, many measures include flexibility for providers to implement them in a cost-effective way that is appropriate for their specific context.

1.159 We have not recommended measures depending on service providers' access to technical expertise. We recognise that service providers need to have access not only to financial resources but also to any technical expertise necessary to implement our measures. Providers could address lack of technical expertise by hiring or contracting for it (provided there are sufficient financial resources to do so). Therefore, we consider that it is a service provider's access to financial resources that ultimately determines its capacity to undertake a particular measure.

Determining whether a service is 'large'

Defining a 'large' service as one with over seven million monthly UK users

1.160 We have decided to retain our definition of a 'large' service as one with more than seven million monthly UK users. This is roughly 10% of the UK population, and broadly equivalent to 'services with a large user base' in the Register. This approach of taking user base as a proxy for the size of service is similar to that adopted by the EU in the DSA.[132] We consider it beneficial to broadly align our approach to determining larger services with other international regimes where possible as this will reduce the potential burden of regulatory compliance for service providers.

1.161 Where we consider it appropriate, we have used a different threshold for individual measures. For example, we consider it appropriate to user a lower threshold when considering the benefits and costs of the CSAM hash-matching measure.

---

[131] Content moderation is an important source of information for a service provider in identifying risks and understanding if they are being effectively managed. The recommended measures will promote consistency in approach to content moderation and reduce the risk of potentially illegal content being missed in the content moderation system.

[132] The DSA classifies platforms or search engines as very large online platforms (VLOPs) or very large online search engines (VLOSEs) if they have more than 45 million users per month in the EU, a number equivalent to 10% of the EU population. Source: Preamble 76, DSA 2022.

1.162 We consider it unlikely that the costs of online safety regulation for most large service providers will be big enough to incentivise them to split their services artificially to evade regulation. We note that this risk could also be said to arise because of the DSA, and we are not aware of it leading to such problems.

1.163 That said, we recognise that user base is not a perfect proxy for access to resources. However, if, as suggested by some stakeholders we were to apply measures based on the revenue of the provider of a service, providers could choose to withdraw a service instead of increasing the resources allocated for it. This is especially likely where a service is tangential to the provider's main business. For example, many companies, such as banks, utilities, and manufacturers have U2U customer forums. There may be more of a risk of services like these being withdrawn if we were to impose onerous obligations on them. This could harm users if the risks of illegal harms posed by such services were low relative to the value they bring.

1.164 Another option might be to consider the revenue of the specific service. However, current revenue (and even profit) may not always accurately capture whether a service has access to resources. Expected future profits can be more important than a service's current financial situation. Therefore, a provider may fund safety improvements on a service that is currently making a loss because it anticipates a future strong revenue stream due to a high user base (even though it is not yet fully monetising that user base).

1.165 On balance, we consider user base to be a reasonable (although imperfect) proxy for access to resources. We also consider it will be relatively simple for most services to determine if they are 'large' or not based on user numbers (see from paragraph 1.175).

Definition of 'user' used to determine if a service is 'large'

1.166 We need to specify how user numbers are calculated for determining if a service is 'large'. For some measures, we must use the definition of 'user' found in the Act. For example, all users (and other affected persons) must be able to easily report content under the Act, and measures relating to this must use the Act's definition of a 'user'. While we have discretion over who should count as a 'user' for the purposes of determining if a service is 'large', it would be simpler to understand the Codes if they have a single definition. For calculating whether a service is large, we therefore want to use a definition of 'user' consistent with the Act.

1.167 Independent of Ofcom's development of Codes, the Secretary of State is laying before Parliament a draft statutory instrument to set thresholds for determining which services are categorised under the Act.[133] Providers of categorised services will have additional obligations, which depend on whether the service is Category 1, 2A or 2B. As part of the criteria for determining if a service is categorised, this draft statutory instrument includes provisions on determining user numbers. DSIT shared a draft of the statutory instrument with us. This specifies how this calculation should be done in a way that is similar to our proposal in the November 2023 Consultation. Part of the proposed criteria for Category 1 and 2A involve thresholds of seven million 'active United Kingdom users'.

[133] This is called 'The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025 draft statutory instrument for categorisation'.

1.168 We have decided to broadly align our calculation of user numbers for determining if a service is 'large' for the purposes of Codes with the calculation of active United Kingdom users in the draft statutory instrument. This is for the following reasons:

a) It uses a definition consistent with the Act.
b) Aligning to the calculation in the draft statutory instrument should avoid confusion and reduce the burden on providers. Some providers will need to calculate their user numbers for the purposes of determining if they have categorised services. It will be simpler for them if they do not need to make a separate calculation for the purposes of determining if they are 'large' for the purposes of the Codes.
c) We consider the calculation in the draft statutory instrument to be reasonable and it is similar to what we consulted on. We do not agree with those responses which argued that service providers should have flexibility to define 'users' as registered users only (or some other, narrower, definition of 'user'). All users can be affected by illegal content, even if they are not registered on a service, so we prefer a wide definition. Having a broad definition of 'user' also ensures consistency between services. If we were to allow providers flexibility to use their own definitions, it would be possible for them to design the definition to avoid applying measures when we consider those measures appropriate.
d) Contrary to some responses, we do not consider this definition to be overly burdensome for service providers. We discuss this further in paragraph 1.175 and 1.176.

1.169 In aligning with the draft statutory instrument, we are assuming it will be passed consistent with the draft that DSIT have shared with us. If this were not to pass, we may need to reconsider our definition in the Codes.

1.170 The calculation of user numbers is set out in our Codes. The main difference compared to our November 2023 Consultation is that the period over which the calculation is done is six months rather than 12 months.

1.171 Some responses asked for more clarity on the definition of user and the calculation. We consider the definition in the draft statutory instrument to be sufficiently clear. Addressing some of the points raised in responses, the definition of active UK user and calculation mean that for a U2U service:

a) A user must access the U2U part of the service to be an active user. To classify as having accessed the U2U part of a service, it is not necessary for the user to post or upload content. Merely viewing (or otherwise encountering) U2U content on a service counts as actively using that service.
b) An active UK user does not have to be registered with a service (consistent with Section 227(2) of the Act).
c) Registered users of a U2U service who do not access the service in a particular month will not count as active users for that month.

1.172 Separate to how user numbers are calculated, we also say in Codes that once a service has met the threshold for being large, it will continue to be treated as large until its user numbers have been below the 7 million threshold for a continuous period of six months. This is to provide additional clarity for providers by reducing the extent to which the status of services can change over time. We consulted on this and there were no comments on it in responses. This is different from the approach envisaged in the draft statutory instrument, which just relies on the calculation in the previous six months.

1.173 We acknowledge the advantages of having as much alignment as possible with online safety regimes in other jurisdictions. At a high level, the definition of user we have adopted is similar to that in the DSA.[134] Both definitions include those who post content and those who view content, and both include non-registered users. However, to the extent there are differences in the details of the definitions and the calculations, we consider it more important to align with the definition of 'user' in the Act and to broadly align with calculation in the draft statutory instrument, than with the definition of 'user' in the DSA.

Difficulty of calculating users

1.174 We agree with responses which said that our definition of 'user' means some service providers will find it difficult or impossible to determine user numbers in a way that is completely accurate. For example, some providers will not be able to tell if the same person accesses a service from different devices, leading to this person being counted multiple times when they should only be counted once.[135] Some providers will therefore need to estimate user numbers rather than using an actual figure.

1.175 Unlike the DSA, we are not requiring all service providers to publish estimates of their user numbers. Most providers will need to do little work to determine if their user base is more or less than seven million monthly UK users. Providers of large services that are confident their service has a user base of over seven million monthly UK users will not need to do any further work, as they can simply assume their service is 'large' for the purposes of applying the Codes.[136]

1.176 Similarly, most providers will be able to confidently decide they have far fewer than seven million monthly UK users of their services, with very little work. For example, a service accessed by significantly less than seven million unique monthly visitors will generally not be 'large'.

1.177 A small number of providers that have services likely to have a monthly UK userbase close to the seven million threshold will need to make a more precise estimate. Some of these providers will, in any case, need to estimate user numbers as part of the processes for determining if they are categorised services under the Act. We would expect them to rely on the same user number estimates for determining if they are large services. Providers may also make use of estimates from third parties (where these are reasonably expected to be sufficiently accurate). For example, we publish data that may be indicative of whether some services are likely to be large services (though care is needed in interpreting this data).[137]

---

[134] In the DSA, an active recipient of an online platform "means a recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface". Source: Article 3(p) of the Digital Services Act 2022. The search definition refers to recipients who have submitted a query Article 3(q).

[135] Conversely, if the same device is used by many different people, then the number of devices may understate the number of users. This effect will usually be smaller than the other effect.

[136] Google asked for the option to 'self-certify' that it meets the relevant threshold without needing to provide user counts (Google response to November 2023 Consultation, p.30). This was to avoid an unnecessary burden of estimating user numbers. A provider does not need to 'certify' its service as being large, but if it considers its service has more than seven million users, then it would need to adopt all relevant measures recommended for a large service to take advantage of the safe harbour. Therefore, providers are effectively able to do what Google suggests.

[137] Ofcom, 2024. Large services: Ipsos Iris data on service reach. [accessed 4 November 2024].

1.178 More service providers will need to calculate user numbers if they are high risk for certain kinds of harm. For example, providers of some services that are at high risk for image-based CSAM will need to estimate their user numbers if they are close to the measure-specific threshold of 700,000 monthly UK users.

Search services

1.179 In April 2024, we wrote to relevant stakeholders clarifying that while a downstream general search service itself will always be in scope of the Act, there is a factual question about which entity involved is the 'provider' of that service, and that this must be determined on a case-by-case basis. The Act explains that "the provider of a search service is to be treated as being the entity that has control over the operations of the search engine (and that entity alone)." It defines "operations of the search engine" as those which "(a) enable users of a search service or a combined service to make search requests, and (b) generate responses to those requests".

1.180 In our April 2024 letter, we explained that in some cases, the upstream entity which provides the index will have control over the "operations of the search engine" and in those cases it would be the 'provider' of the downstream service for the purposes of the Act. However, there may be circumstances in which the downstream entity exercises control, and in those circumstances the downstream entity would be the 'provider'.

1.181 We received feedback to our April 2024 letter that evidenced the ongoing complexities of, and variations within, different syndication partnership. [✂].[138]

1.182 How the Act applies to the specific position of each entity involved in a search service is a matter for the entity to consider for itself. We recognise that there are complexities associated with the downstream search business model which may make it more difficult to determine who the provider is. Ultimately, the entities involved in such an arrangement are best placed to make the determination as to, firstly, how many distinct search services are being offered to users, and, secondly, who the 'provider' is for each of these services, based on the specific contractual and technical arrangements underpinning the relevant service. In cases of doubt, we expect both parties to seek legal advice and enter appropriate commercial arrangements that secure compliance with the Act. For example, while the provider of a downstream general search service will be legally responsible for ensuring compliance with all safety duties, we understand it may be necessary to delegate some of the operational tasks relevant to these regulatory duties to the other entity involved in the downstream general search service if that entity is better placed to ensure a particular measure (or equivalent system or process) is implemented effectively.

1.183 If entities involved in a downstream general search service arrangement fail to agree on who the 'provider' of the service is, each entity risks being determined as the 'provider' by us (and thus held liable for breaches of the duties under the Act in any resulting enforcement action).

Functionality and service type

1.184 When proposing measures for our Codes, we have looked to ensure proportionality across the range of services captured by the Act, as detailed in our discussion of design of our measures and our impact assessment process.

[138] [✂].

1.185 Our measures apply to the 'provider' of the service as defined in the Act, regardless of the type of service. Where more than one person has a role in relation to the provision of a regulated service, there may be uncertainty which one is the 'provider' of the service. It is for the persons concerned to manage this risk, where appropriate by taking legal advice, in order to ensure that the duties are met.

1.186 For decentralised and VR services, we consider that our measures are sufficiently flexible to work. In line with our November 2023 Consultation, nothing we are doing is asking providers to break encryption.