WARNING: This consultation response contains language and/or material that may be distressing

Consultation response form

Please complete this form in full and return to protectingchildren@ofcom.org.uk.

Consultation title	Consultation: Protecting children from harms online
Organisation name	Canadian Centre for Child Protection Inc.

Your response

Question	Your response
Volume 2: Identifying the services children are using **Children's Access Assessments (Section 4).**	
Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view. 1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance? 2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met? 3. Our proposed approach to the process for children's access assessments?	Confidential? – NO As an overarching statement for our responses below, the assessment of whether a service is "likely to be accessed by children" is critical and must be done in a way that scopes in services that present a risk to even a few children. In our view, every service should be required to have basic safety, governance and accountability measures to help keep children safe online. We recognize that under the Online Safey Act, the duties regarding child's risk assessments and protecting children's online safety apply to services that are "likely to be accessed by children". We believe that it is fundamentally flawed to permit certain services to have zero child-safety measures, and this may leave gaps that those seeking to harm children exploit. However, considering this limitation is set out in the legislation, we will focus our responses on how children's access is assessed. We wish to emphasize paragraphs 4.22 – 4.24, and are supportive of Ofcom's position that "even a relatively small absolute number or proportion of children could be significant in terms of the risk of harm to children". 1. On the surface the proposal is reasonable – that a company should only conclude their service is not accessible by children if they are using highly effective age assurance. The strength of this proposal relies on how highly effective age assurance is defined and the steps needed for a company to demonstrate the process they've employed is highly effective. There has been some significant thought put into highly effective age verification in Annex 10. Our concern is that too much trust may be put into Facial age estimation at this time. Our understanding is that although claims by companies producing the algorithms/software for these tools show they are highly effective, there are still

Question	Your response
	questions about its effectiveness, particularly if it is used as the sole method for verification. NIST Reports First Results From Age Estimation Software Evaluation | NIST FTC denies facial age estimation as verification tactic | GamesIndustry.biz We have also had direct experience with being able to get past age estimation tools. Example: the platform, Wizz, uses age estimation tools to “ensure” only children are on the platform. Female Cybertip.ca analysts who were 23 and 25 years old went through the facial recognition process and were able to create accounts on Wizz as 16 year old males. The Wizz account set up process included entering an email/Apple ID, “date of birth”, face scanning using Yoti, and uploading photos to the profile (the photos did not have to match the face scanned). Users were then able to choose if they want to see other users from their country, or worldwide and the age range of users they’d like to see. We tested the efficacy of this process following a mass increase of reports to Cybertip.ca concerning sextortion of youth. https://www.cybertip.ca/en/online-harms/alerts/2024/wizz-app/ 2. See opening paragraph. 3. Both research and media reports will be critical in determining the accuracy of access assessments. Media reports are important to challenge those that may suggest that they have highly effective age assurance. OnlyFans markets itself as an 18-plus only digital media platform - yet stories like the one from Reuters challenges that notion. https://www.reuters.com/investigates/special-report/onlyfans-sex-children/ We know Ofcom has started an investigation into their age assurance claims as well. Independent research and media reports from investigative journalists offer an important lens into potential gaps and risk to children. Other considerations/concerns:

Question	Your response
	- Social media services that allow pornography (X/Twitter) or search engines that provide open access to pornography - will they be covered under Part 5 as a regulated provider of pornographic content? Twitter itself estimates that as much as 13% of content on its platform is adult pornography. - 4.27 contains a footnote for the ICO's Guidance: Likely to be accessed by children. In reviewing the former guidance, C3P is concerned by the use of the word "decide" instead of "assess" in two statements particularly: *- You should **decide** whether children are likely to access your service, even if you run an adult-only service.* - *As a provider of an Information Society Service (ISS), you should **decide** whether all or part of your service falls within scope of our Children's code.* - 4.32 references a "table 7" in "guidance" for a list of factors to consider when carrying out the assessment of the child user condition – a table numbered in this manner doesn't appear in the referenced link to the ICO's guidance page
Volume 3: The causes and impacts of online harm to children **Draft Children's Register of Risk (Section 7)**	
Proposed approach: 4. Do you have any views on Ofcom's assessment of the causes and impacts of online harms? Please provide evidence to support your answer. a. Do you think we have missed anything important in our analysis? 5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer.	Confidential? – NO **4.** Ofcom presents numerous examples of the causes and impacts of online harms, many which we observe on a regular basis. In our 2019 framework document we describe similar examples, notably the use of "legal" excerpts from known series of child sexual abuse material. These forms of harm are why online safety, and safety by design requirements need broad application and where strong classification efforts combined with proactive detection are necessary with service providers. **5.** We are maintaining a "Track record of online harm", this compilation of public reports is documenting the failures and concerning behaviours exhibited by technology companies, including social media platforms.

Question	Your response
6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer. 7. Do you have any views on our interpretation of non-designated content or our approach to identifying non-designated content? Please provide evidence to support your answer. **Evidence gathering for future work:** 8. Do you have any evidence relating to kinds of content that increase the risk of harm from Primary Priority, Priority or Non-designated Content, when viewed in combination (to be considered as part of cumulative harm)? 9. Have you identified risks to children from GenAI content or applications on U2U or Search services? a) Please Provide any information about any risks identified 10. Do you have any specific evidence relevant to our assessment of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in: a) (i) specific examples of body image or depressive content linked to significant harms to children, b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content. 11. Do you propose any other category of content that could meet the definition of NDC under the Act at this stage? Please provide evidence to support your answer.	In addition, in our response to the third phase consultation relating to additional duties for categorized services we included the following publications for consideration: • Kerr, S & Kingsbury, M. (2024). Online digital media use and adolescent mental health. https://www150.statcan.gc.ca/n1/en/pub/82-003-x/2023002/article/00002-eng.pdf?st=MlOoEIcO • NSPCC (2023). Online risks to children: Evidence review. https://learning.nspcc.org.uk/research-resources/2023/online-risks-to-children-evidence-review • U.S. Attorney General's Advisory (2023). Social Media and Youth Mental Health. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf • Molly Rose Foundation. (2023). Preventable yet pervasive: The prevalence and characteristics of harmful content, including suicide and self-harm material on Instagram, TikTok and Pinterest. https://mollyrosefoundation.org/wp-content/uploads/2023/11/Preventable-Yet-Pervasive-MRF-TBI-Nov-23.pdf • Center for Countering Digital Hate. (2022). Deadly by design: TikTok pushes harmful content promoting eating disorders and self-harm into young users' feeds. https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf • Thorn. (2022). Online grooming: Examining risky encounters amid everyday digital socialization. Findings from 2021 qualitative and quantitative research among 9-17-year-olds. https://info.thorn.org/hubfs/Research/2022_Online_Grooming_Report.pdf • Ofcom. (2022). Research into risk factors that may lead children to harm online. https://www.revealingreality.co.uk/2022/10/11/research-into-risk-factors-that-may-lead-children-to-harm-online/ • WeProtect. (2021). Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18 to 20 years old. https://www.weprotect.org/economist-impact-global-survey/#report • Stoilva, M., Livingstone, S. & Khazbak, R. (2021, February). Investigating risks and opportunities for

Question	Your response
	children in a digital world: A rapid review of the evidence on children's internet use and outcomes. Unicef. https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf • Katz, A., & El Asam, A. (2021). Refuge and risk: Life online for vulnerable young people. Internet Matters and Youthworks. https://www.internetmatters.org/wp-content/uploads/2021/01/Internet-Matters-Refuge-And-Risk-Report.pdf • UNICEF. (2021). Investigating Risks and Opportunities for Children in a Digital World. https://www.un-ilibrary.org/content/papers/10.18356/25211110-2020-03 **6.** Nothing further to add. **7.** The statement and sentiment in 7.9.15 (excerpt below) appear in other sections, the concern we would highlight relates to the idea of "appreciable number of children" *'Appreciable number of children' is defined further in the Act's explanatory notes, which state that content "need not adversely affect a very large number of children" to be classified as harmful content. However, content which may adversely affect "only one child or very few children" should not be defined as 'content harmful to children'* Our recommendation for the regulator is to take a very narrow view on the threshold of "very few". Evidence in this consultation shows children have broad access to harmful content and adult content and services. If something can be accessed by even one child it can be accessed by many and should be designed and protected accordingly. **8.** We are aware of several media reports describing harm experienced by children that resulted from their ability to access content that led to the exposure of Primary Priority Content and Priority Content. For example:

Question	Your response
	• Horror and gore related content: https://www.washingtonpost.com/investigations/interactive/2024/764-predator-discord-telegram/ • Cartoon Pornography: ￼https://endsexualexploitation.org/articles/cartoon-pornography-a-serious-threat-to-our-children/ (we note 8.2.11 stating that artificial pornography is considered PPC – this article is useful to illustrate how exposure to cartoon pornography is impacting children) • Pornography; https://mediasmarts.ca/sites/default/files/2023-01/Encountering%20Harmful%20and%20Discomforting%20Content%20Report%20-%20YCWW%20Phase%20IV.pdf https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf **9.** We are seeing increasing risks to children relating to Generative AI. The IWF's October 2023 report "How AI is being abused to create child sexual abuse imagery" is a good online account of the risks we are observing including the generation of images of known victims and children known to offenders in real life. In Canada, we have been involved in reports of children using Generative AI tools to produce intimate images of peers. Similar cases have been observed in the United States and Spain: • https://www.cbc.ca/news/canada/manitoba/artificial-intelligence-nude-doctored-photos-students-high-school-winnipeg-1.7060569 • https://globalnews.ca/news/10073305/ai-nude-images-deepfakes-westfield-high-school-classmates-new-jersey/ • https://www.theguardian.com/world/article/2024/jul/09/spain-sentences-15-school-children-over-ai-generated-naked-images We have created high school lessons to support high schools (Gr 9-12) with education tools addressing AI-related concerns and have also amended middle

Question	Your response
	school lessons (Gr 7/8) to include deepfake/AI related issues.We are continuing to develop education and diversion techniques as we believe those are much more effective than criminal approaches. We also support researchers like those at Stanford on better understanding of the child sexual abuse material contained within some of the better known models, reference Stanford Report and the discovery of CSAM in the LAION models (https://cyber.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse).Ofcom may consider reviewing the following publications: • UNICEF: “*Generative AI: Risks and Opportunities for Children*”. https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children • The Canadian Standards Association Group: "*Children’s Privacy in the Age of Artificial Intelligence*". https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Children_s-Privacy-in-the-Age-of-Artificial-Intelligence.pdfChild Rescue Coalition: *“The Dark Side of AI: Risks to Children”.* https://childrescuecoalition.org/educations/the-dark-side-of-ai-risks-to-children/ • Common Sense Media: *“AI Initiative”*. https://www.commonsensemedia.org/ai • Caroline Mimbs Nyce: *“A Generation of AI Guinea Pigs”* https://www.theatlantic.com/technology/archive/2024/06/kids-generative-ai/678694/ • Joint Committee on Children, Equality, Disability, Integration and Youth debate: *Protection of Children in the Use of Artificial Intelligence: Discussion. https://www.oireachtas.ie/en/debates/debate/joint_committee_on_children_equality_disability_integration_and_youth/2024-02-13/2* **10.** Nothing to add. **11.** Nothing to add.
Draft Guidance on Content Harmful to Children (Section 8)	

Question	Your response
12. Do you agree with our proposed approach, including the level of specificity of examples given and the proposal to include contextual information for services to consider? 13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children? 14. For each of the harms discussed, are there additional categories of content that Ofcom a) should consider to be harmful or b) consider not to be harmful or c) where our current proposals should be reconsidered?	Confidential? – NO **12.** Providing specific examples and contextual information is important to help services understand the ways children can be harmed. Context can be the primary factor in determining harm in certain circumstances. One example central to the work we do is the use of a known victim's image in a completely safe and normal setting. To the average person this image has no deeper meaning, but to a victim and the offending community this same image is a signpost to image of the abuse that has been inflicted on the child. **13.** Nothing additional to share **14.** Any additional categories would be contained with C3P's Child Protection and Right Framework (already mentioned within this document).
Volume 4: How should services assess the risk of online harms? **Governance and Accountability (Section 11)**	
15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 16. Do you agree with our assumption that the proposed governance measures for Children's Safety Codes could be implemented through the same process as the equivalent draft Illegal Content Codes?	Confidential? – NO 15. Our responses to Volume 3 Governance and Accountability of the Illegal Harms Consultation (specifically responses to Questions 3 and 7) are relevant to this consultation and response. ALL services should be required to meet basic children's safety requirements. **As was the case in our Illegal Harms Consultation a key theme in our responses is that basing child safety proportionally on the popularity of a product does not exist in the physical world, and should not exist online. Services should be scoped in based on risk and functionality, not size.** Exempting services based on size, risk, the presence of age assurance or the number of children accessing the service results in a piecemeal approach when what is needed are base-level requirements and expectations for child safety online that foster a culture of safety and care. Many of the proposed governance measures only apply to large or multi-risk companies. The focus on

Question	Your response
	"multi-risk" services misguided is in this context. Each type of PPC and PC is harmful on its own. There are services dedicated to a single type of PPC or PC. For example, pornography sites or eating disorders websites. These sites may be not large or multi-risk, yet the individual harm to children of exposure to any one type of PPC or PC through the service warrants a robust child safety approach. As to platform size, in Illegal Harms Consultation responses (see especially our response to Question 8) we provided Omegle (no longer operating) and Wizz as examples of services that are unlikely to meet the threshold of 7 million UK users but pose a significant risk to children. It is unacceptable for these platforms like these to be exempt from the annual review (GA1) and internal monitoring/assurance measures (GA4). Additionally, some platforms are aimed at, or have sections aimed at, children such as Chat Avenue's Teen Room. Such platforms will have smaller user bases because children are a minority segment of the population. Effectively, platforms aimed at children will be exempt from the full slate of governance measures until they have a user base of 7 million, which is nearly half of UK children. It is illogical that platforms could be developed for children, yet not be required to conduct annual child safety reviews and have internal monitoring and assurance functions. We do not agree with certain assumptions in Volume 4, such the statement in paragraph 11.188 that smaller, single-risk services "are more likely to be able to achieve an adequate level of understanding among relevant staff through informal means". In our experience, platforms do not consider or understand child safety, and are focused more on growing their userbase and technical capacity. For example, most of responsible for internet start-ups do not have a background in child development and may not understand broader online ecosystem in which harm to children is occurring. If there are no or limited regulations for smaller, "single-risk" platforms, it is likely that many of these companies will encounter the

Question	Your response
	same issues and make the same the mistakes while children are harmed in the process. We do not exempt smaller companies in other regulatory contexts. To address concerns about the burden on smaller companies, the regulator could consider developing resources such as: - Online training modules for staff at smaller companies. The modules could include quizzes to demonstrate knowledge and could be designed to issue a record of completion that the individual/company should keep on file. There are various examples of regulators developing trainings in other settings. For example, the Canadian province of Manitoba has accessibility legislation, and the Manitoba Accessibility Office is responsible for public education/awareness of the legislation. This office provides free online training that helps employees understand their responsibilities under the legislation. A certificate of completion is issued at the end. - The regulator could look at developing a helpline for companies that have questions about their responsibilities. It could provide guidance from the regulator or help connect companies to other resources. The following addresses how we believe each governance measure ought to apply: - GA1: Annual review of risk management. The requirement for some level of scaled (depending on size / overall risk) review of risk management activities, occurring annually, should be placed of any online platform. This will promote a culture of child safety and help ensure there is a process in place for when access by a child occurs, at which point prevention and mitigation steps can be taken. The annual review process currently reserved for large platforms could be scaled down for smaller platforms. For example, instead of requiring the "most senior body" to carry out the annual, it could be the most senior person. - GA2: Accountable person. If it is possible under the Online Safety Act, all companies should be re-

Question	Your response
	quired to assign a person accountable on the issue of child safety, even if the service is not assessed as “likely to be accessed by children”. Any platform is at risk of being accessed by a child; someone should be responsible for considering that risk, and responding if it does occur. It could be the same person responsible for the annual children’s access assessment. - GA3: Written statements of responsibility. This measure should be required for smaller and single-risk services. Assigning responsibility is a basic yet important measure for promoting child safety. - GA4: Internal monitoring and assurance. There should be an adapted requirement for smaller or single-risk companies to have some tracking and review of their mitigation measures. - GA5: Tracking evidence of new and increasing harm. In addition to the considerations of this accountability measure, the regulator should consider how investments made by larger services to improve tracking / monitoring activities can be leveraged to support smaller services. Alternatively, Ofcom should consider sourcing and / or funding solutions for smaller services to utilize. - GA6: Code of conduct regarding protection of children from harmful content. As we have previously submitted, a code of conduct is a basic obligation in many other contexts and will help promote safer company cultures. The code of conduct could be as simple as a one-pager that makes employees aware of the company’s commitment to child safety. This is the foundation of creating organizations that embrace a safety by design approach to products and services; without this basic commitment child safety becomes an afterthought. Ofcom could provide a sample Code for companies to adapt. - GA7: Staff compliance training for staff involved in the design and operation of a service. This measure should apply to all user-to-user and search services full stop. If a service is explicitly adult in nature it should be an industry leader in age or user verification to protect children prior to engaging with the service. Only with the combination of

Question	Your response
	GA6 (code of conduct) and child safety compliance training will you have a true safety by design mentality with online services. Smaller, single-risk companies are currently exempt from GA7. However, individuals running smaller companies do not understand child safety risks and the ways in which their service may be misused. At least some training is needed. 16. Yes, we believe the governance measures and related processes for Illegal Harms and Children's Safety can be one and the same. Further to that point our overall belief is that there does not need to be a distinction at all between the two types of protections and as has been stated size of a service's user base should not be a deciding factor on whether children's safety is a cost of doing business.
Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)	
17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. 18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. Specifically, we welcome evidence from regulated services on the following: 19. Do you think the four-step risk assessment process and the Children's Risk Profiles are useful models to help services understand the risks that their services pose to children and	Confidential? – NO **17.** Overall, the risk assessment process appears robust, and the Children's Register of Risks captures many important factors. It will be critical for this register to continue to evolve as new risks emerge – as noted above, reference to media and research (including NGO reports) will be critical. Paragraph 2.19 of Annex 6 indicates that a risk assessment must be carried out within 3 months of starting a new service or changing an existing service so it falls within the scope of the Act for the first time. All risk assessments should be done at the outset, prior to launching any changes. Many online services launch first, and consider safety second. Safety should be part of the design process, and the risks should be considered out front. The proposal in 2.20 requiring services to keep their assessments up-to-date and carry out further assessment before making a significant change is positive. **Further to the overarching sentiment of our remarks, we recommend the broadest interpretation for requiring basic Risk Assessments.** Step 1 of the Children's Risk Assessment is outlined in Volume 4, point 12.2 - "Service providers must first carry out a

Question	Your response
comply with their child risk assessment obligations under the Act? 20. Are there any specific aspects of the children's risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft? 21. Are the Children's Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service? a) If you have comments or input related to the links between different kinds of content harmful to children and risk factors, please refer to Volume 3: Causes and Impacts of Harms to Children Online which includes the draft Children's Register of Risks.	children's access assessment to understand if their service, or part of their service, is likely to be accessed by children. The duty to carry out a children's risk assessment arises for user-to-user ('U2U') and search services, or parts of these services, that are likely to be accessed by children." This step prematurely limits responsibility for children's safety. Given the minimum requirements and basic obligations for ALL services to have in place for illegal content we propose those same minimum requirements for as many services as possible to ensure a basic understanding of Children's Safety so that, at a minimum, **services have basic analysis and reporting functions in place so some action can be taken when a child accesses their service**. **Risk Assessments should be for as many services as possible** – "suitable and sufficient" are the obligations for risk assessments in the Act, and are sufficiently broad to be adapted to different scenario. The Risk Assessment rationale recognizes no one-size fits all approach exists due to a multitude of risk factors. **In our response to Illegal Harms governance and accountability, we proposed two fundamental priorities that should matter for all online services, regardless of size (12.42 - 12.49). These priorities include: <u>ZERO TOLERANCE FOR ILLEGAL MATERIAL</u>, and <u>CHILD SAFETY IS A PRIORITY</u>.** In 12.76 the consultation rationalizes associated costs as being "outweighed by the significant benefits arising from obtaining and considering these inputs and to be necessary to improve the quality of the risk assessment where needed." This is the fundamental point about the cost of doing business. Service providers must be aware of potential risk and have appropriate steps in places to address them. **18., 19., 20., 21. See our responses to <u>Volume 3 Governance and Accountability of the Illegal Harms Consultation (specifically responses to Questions 8, and 9)</u>**
Volume 5 – What should services do to mitigate the risk of online harms **Our proposals for the Children's Safety Codes (Section 13)**	

Question	Your response
Proposed measures 22. Do you agree with our proposed package of measures for the first Children's Safety Codes? a) If not, please explain why. **Evidence gathering for future work.** 23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration? a) If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures. 24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes? a) If so, please explain why and provide supporting evidence.	Confidential? – NO **22.** These measures provide a good starting point to ensuring that children are not exposed to harmful content online. We have been advised that all activities in this consultation are qualified by "likely to be accessed by children". As stated above, we firmly support the notion that ALL services should be required to meet some basic child-safety obligations. As with our submission to the Illegal Harms Consultation, a key theme in our responses continues to be the notion that basing child safety proportionally on the popularity of a product does not exist in the physical world and should not exist online. There are several examples of very small service providers that have an incredibly outsized impact on harm. These often include file hosting services or fast-growing startup social networking applications. There needs to be flexibility in the legislation/regulations to ensure these edge cases can be scoped in as needed. Canada's recently announced legislation contemplates bringing smaller companies into scope once risk is established. In the case of this consultation the limitation on services that are "likely to be accessed by children" should not prevent basic child safety considerations for all services. As a result, we believe that the proposed measures can go further by applying the measures more broadly. See our response to Question 3 in our Illegal Harms Consultation submission for a full explanation of our concerns regarding the application of measures on the basis of size. We are also concerned about the degree of discretion being given to service providers in determining how they will implement several of the Children's Code measures. As noted in our responses to follow (questions 46, 47, and 54) there are areas that we believe that Ofcom can take a more prescriptive approach in their expectations of how service providers will fulfil these measures while still allowing service providers the flexibility to tailor these measures to their services.

Question	Your response
	Paragraph **13.34**: We feel that the absence of a requirement for service providers to make use of automated detection tools leaves a major gap in the ability for service providers to prevent children from encountering harmful content. Such a measure should be considered an expectation on all U2U services, especially large services. On these services, it not feasible that the detection and review of harmful content be left solely to human moderation. Further, we cannot rely on the notion that some "large services often do so". While this may be true, we have witnessed many large service providers, including those that make use of these systems, fail to protect children from harmful content. **Q.23.** C3P's tech harm timeline highlights copious examples of where service providers are failing to meet basic safety measures. Also see our responses in Volume 4. **Q.24.** Nothing to add.

Developing the Children’s Safety Codes: Our framework (Section 14)	
25. Do you agree with our approach to developing the proposed measures for the Children’s Safety Codes? a) If not, please explain why. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content? a) Please explain your views. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children? 28. Do you agree with our definition of ‘large’ and with how we apply this in our recommendations? 29. Do you agree with our definition of ‘multi-risk’ and with how we apply this in our recommendations? 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?	Confidential? – NO **25.** See our response to Question 22 of this document. The limitations placed on service providers that are “likely to be accessed by children” and the application of measures based on size and risk (multi-risk, low-high risk) should be broadened to ensure that ALL services are required to meet basic children safety obligations. We also hope that Ofcom will clarify which of their proposed actions are expectations (requirements) or recommendations. For example, it is noted that service providers “should” undertake a certain policy or make a certain feature available to users. In most cases it is clear these refer to Ofcom’s expectations of service providers. In some cases, however it is unclear whether these are an expectation or simply a recommendation. For example, paragraph 16.268 states “*Service providers **should** also ensure that the materials are clearly labelled and easily accessible, so that volunteer moderators are aware of their availability.”* While related to measure CM7 (we suggest that should be applied to CM6) it is unclear whether Ofcom expects service providers to do this to fulfil this measure, or whether this is a recommended practice. Another example where it is unclear whether a certain practice is an expectation or recommendation is located in paragraph 21.28. Specifically, “*The message **should** include any relevant publicly visible information about the user inviting the child to join, as well as such information about the group*.” While relevant to measure US1, it is not clear whether service providers are expected to include this information to fulfil their duty under this measure. **27**. See our Illegal Harms Consultation submission (specifically Question 3). **28.** See our Illegal Harms Consultation submission. We believe the application of “large” limits the application and intention of several measures proposed in this consultation. As stated in our Illegal Harms Submission and response to the question on Volume 4, services aimed at children are likely to have smaller user bases and are less likely to meet a user threshold that is based on the entire population.

	While there are several, we would like to highlight a couple examples of services that would not likely meet the threshold to be considered “large” consistent with Ofcom’s definition: 1) Wizz: this service is a chat app owned by a Paris-based company aimed, according to its website, at 13-24 year olds (see https://wizzapp.com/our-safety-strategy/). The app permits users to swipe through profiles (like how some dating apps work) and chat with strangers. Cybertip.ca has received 180+ reports concerning Wizz since 2021, leading to a Cybertip.ca Alert in early 2024. As stated in the alert, compared to 2022, we received 10 times as many reports about the app in 2023. Reports about Wizz increased faster than any other platform. Most reports concerned sextortion involving male victims. The majority of victims reported to Cybertip.ca were between 15 - 17 years old. The app has 15 million users worldwide. ￼ 2) Monkey: this service is similar to Omegle in that it allows users to choose which gender they want to chat with and how many people (either a group or individual). The platform is marketing itself as an alternative to Omegle, stating that: “Monkey stands out as the top choice for those seeking the best Omegle alternative app”. Monkey purports to have 30 million users worldwide. While the terms of service states that users must be 18 to use the app, there are no robust measures to ensure that users are in fact 18 or older, instead relying on a self-reported age (age gate). Despite this, Cybertip.ca has received several reports from minors who were sextorted on this service. To further our comments on the definition of “large” regarding service size, in a submission to the eSafety Commissioner, we stated that even a threshold of 500,000 monthly users would be too great for hosting services. https://www.esafety.gov.au/sites/default/files/2024-02/standards-submission-from-Canadian-Centre-for-Child-Protection_0.pdf?v=1718654452464 **29:** Content moderation measures CM2-CM7 are limited to service providers that have a “multi-risk” of content harmful to children. Like other proposed measures we believe these measures (and others) should be applied to services that have the risk of “**one** or more” kinds of harmful content. There should not have to be a risk of multiple harms for children in order for service providers to implement content moderation practices defined in CM2-CM7. It is our view that

	regardless of size and risk, service providers should have in place basic safety obligations, including internal content policies (CM2), well-resourced content moderation teams (CM5), for example.
Age assurance measures (Section 15)	
31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views. a) Are there any cases in which HEAA may not be appropriate and proportionate?	Confidential? – NO 31-32. Yes, we broadly agree with Ofcom's proposals in AA1-AA6. However, we believe that the level of risk needed to trigger several measures in this section must be reconsidered. Unless highly effective age assurance mechanisms are in place, any service is susceptible to access by children. We believe that **all** U2U that pose an established amount of risk (whether low, medium, high or single - multi) that children will encounter content that is harmful should be required to implement highly effective age assurance mechanisms.

b) In this case, are there alternative approaches to age assurance which would be better suited? 32. Do you agree with the scope of the services captured by AA1-6? 33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively? 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services? a) Please provide any supporting information or evidence in support of your views. 35. Do you have any information or evidence on other ways that services could consider different age groups when using age assurance to protect children in age groups judged to be at risk of harm from encountering PC?	Measures AA2, AA4, AA5, and AA6 should extend to services that have even a **low** risk of at least one type of PCC/PC. A medium level of risk is an unnecessarily high threshold, particularly when harmful content is not prohibited on a service. If there is any risk that children can encounter PPC or PC content, service providers ought to ensure this content is not accessible to children. Moreover, levels of risk and size are variable and likely to fluctuate, potentially rapidly. As noted previously, in some cases this can create incentives to disperse services over multiple platforms (see our response to the Illegal Harms Consultation, question 3(i)). Below we provide examples of children encountering harmful content on platforms and services that could be considered "low" or even no risk: We cite the following relevant statistic: *"a majority of all teens (51%) said they have accidentally encountered pornography via clicking a link, a search engine result, an online ad, or on social media in some way. Respondents reported that this accidental online exposure came from a diffuse array of sources: links to websites they did not realize were pornography (including those sent to them by a friend), online ads, search engine results, and social media."* https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf .We further highlight Ofcom's relevant research findings that *"Children reported that it was common for them to encounter violent content that had been uploaded directly to the social media, messaging, and video sharing services they used most frequently, which they said were TikTok, Instagram and Snapchat."* https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/experiences-of-children/understanding-pathways-to-online-violent-content-among-children.pdf Additional examples of children having encountered, or potentially encountering harmful content on low risk services include: https://www.wsj.com/tech/instagram-recommends-sexual-videos-to-accounts-for-13-year-olds-tests-show-b6123c65 https://www.404media.co/how-to-upload-porn-to-instagram/

	https://www.404media.co/inside-the-secretive-world-of-youtube-porn/
Content moderation U2U (Section 16)	
36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – NO 36. Measures CM2- CM7 should apply to ALL user-to-user services, regardless of size or risk. The limitation of these measures to services that are multi-risk does not go far enough to ensure children will not encounter this type of content. As stated previously, we firmly support minimum requirements and basic obligations for ALL services. Measures CM2-CM7 represent minimum safety obligations that all U2U services should adhere to. An example highlighted in our Illegal Harms submission described the clear and uniform food-handling expectations and rules for food establishments whether a small kiosk or a national fast-food chain. In a similar vein, we hope that small-medium services have minimum content moderation requirements to ensure they address and mitigate content that is harmful for children. Proportionality, an ongoing focus of the regulator, can still factor in but within the content moderation activity level. So all services would be capable of content moderation but the level of investment in these areas will be proportional to the need for moderation of regulated content. We believe that measures CM2-CM6 should apply to all U2U services given that the effectiveness of measure CM1 is likely to be contingent on service having in place systems related to CM2-CM6 (internal content policies (CM2), set performance targets (CM3), have and apply content prioritization policies (CM4), well-resourced moderation functions (CM5), and ensure that moderation teams are appropriately trained (CM6)). Regardless of size and risk, **service providers must have sufficient human moderation resources to review and respond to the amount of content on the service and to detect and remove (shield from children) harmful content**. Sufficient resources can be determined based on the level of risk present on the service and its user-base.

	Currently, the expectations surrounding what is considered “well resourced” are unclear. Aligned with a proportional approach, we suggest establishing guidelines for the definition of well-resourced in regard to: • User volume; • User engagement (e.g. volume of user-generated content contributed); • Risk level; • Staffing commensurate with abuse report response time response. **37.** Yes, we agree with the addition of Measure 4G to the Illegal Content Codes which provides explicit direction for training of volunteer content moderators. Volunteer moderators are a reality and if they are to be deployed in a responsible way, they must have the training and materials to do so safely and effectively.
Search moderation (Section 17)	
38. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 39. Are there additional steps that services take to protect children from the harms set out in the Act? a) If so, how effective are they? 40. Regarding Measure SM2, do you agree that it is proportionate to preclude users believed to be a child from turning the safe search settings off? The use of Generative AI (GenAI), see Introduction to Volume 5, to facilitate search is an emerging development, which may include where search services have integrated GenAI into their functionalities, as well as where standalone GenAI services perform search	Confidential? – NO **38.** See question 19 (i) in our submission to the Illegal Harms Consultation. Our response here is similar to our comments regarding measures CM1-CM7, in that measures SM3-SM7 should be expanded so that they apply to all search engines regardless of risk and size. As stated previously, we hope that even small services have minimum requirements to ensure they address harmful content. Basic obligations such as those defined in SM2-SM7 will lead to more consideration of issues during development and help prevent online services from being misused. **40.** We agree that users believed to be children should not be able to turn off safe search settings. However, the use of algorithms to filter out the “most harmful content” from children’s feeds should not be limited to PCC content but also include PC content.

functions. There is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this code. We welcome further evidence from stakeholders on the following questions and please provider arguments and evidence to support your views: 41. Do you consider that it is technically feasible to apply the proposed code measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? 42. What additional search moderation measures might be applicable where GenAI performs or is integrated into search functions?	

User reporting and complaints (Section 18)

43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)? a) Please provide any arguments and supporting evidence.	Confidential? – NO **43.** Regarding paragraph **18.134:** "*we think that providers are best placed to determine which categories of content harmful to children are most appropriate for their particular user base, risks and terms of service.*" We recommend that Ofcom considers recommending or working with industry to build toward a standardized user reporting mechanism, menu and language. Ofcom may consider reviewing the study titled "A comparative analysis of platform reporting flows" by researcher Alex Leavitt (UC Berkeley/Roblox) for a better understanding of this issue. Research conducted by C3P, and observations made through our Cybertip.ca work, have shown that services have failed to provide reporting options that adequately capture the harm occurring on their platforms. In our 2022 report "*An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion*" we found that many victims of sextortion had expressed frustration over reporting menus and options that were not specifically related to sextortion and failed to capture the urgency of the matter when users are being aggressively (and actively) targeted on these platforms. https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf In our 2020 report, "*Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms*", we explained the need for CSAM-specific reporting functions. We found that while the majority of platforms have reporting mechanisms for content at large, they rarely have a CSAM- specific process or menu options for users to report material that is (or believed to be) CSAM. This report also found that on some platforms reporting measures did not allow users to report specific users, user profiles, specific posts, or a combination of the latter. https://content.c3p.ca/pdfs/C3P_ReviewingCSAMMaterialReporting_en.pdf Ofcom may wish to reconsider its decision not to provide service providers a standardized categories of

	content that should be present to users when complaining. Question for Ofcom: are specific users, user profiles, specific posts contained within the definition of content that is users may make a complaint about? **Paragraph 18.311:** *While some service providers currently use trusted flaggers for some illegal content, and we proposed a dedicated reporting channel for trusted flaggers of fraudulent content in our draft Illegal Content Codes, we do not have sufficient evidence on the effectiveness or cost of these programmes for content harmful to children* Illegal Harms Consultation Response question 51(i): In our experience, only a few of the big tech companies have “trusted flaggers” and it is based on their invite/criteria to determine who is trusted. In the context of CSAM and harmful material of children, we recommend considering language like ‘reporting entity or body’ in addition to trusted flagger or clarifying the definition of trusted flagger so it is not based on company discretion. Such a trusted flagger/reporting body system could also be applied to content that is harmful to children. **43b**. Illegal Harms Consultation, see responses to question 28.

Terms of service and publicly available statements (Section 19)	
46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to be included in the Children's Safety Codes? a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 47. Can you identify any further **characteristics that may improve the clarity and accessibility of terms and statements for children**? 48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	Confidential? – NO **46 and 47:** Regarding **paragraph 19.87:** *We considered taking a prescriptive approach to this measure, recommending that services implement specific design criteria to achieve key characteristics of clear and accessible provisions for children. However, given the diversity and complexity of the services in scope of this measure, including their user bases and the design of their services, we do not consider that a prescriptive approach offers enough flexibility to achieve clarity and accessibility of the relevant provisions across these services.* Consider specific standardized requirements for terms of service as a way of ensuring that in-scope service providers adhere to measure TS2. Standardized requirements can be broad enough to allow for flexibility across diverse platforms. For example, it may be recommended (or required) that the ability to access the terms of service and its contents are displayed in a defined minimum font size (this is consistent with measure TS2). As evidenced on many platforms, it is often difficult to locate the terms of service due to both the location on the webpage and the small font size. This is true even when terms of service are made accessible throughout the user experience on an online service. One example of a difficult to access terms of service can be viewed on the web version of Instagram: • The terms of service are located at the bottom of the webpage in small font. • The continuous scroll function on Instagram only allows users to click on the terms of service for a few moments while Instagram's feed loads. When the feed as loaded, the terms of service are pushed to the bottom of the page. Put differently, the continuous scroll function pushes the terms of service to the bottom of screen, in which they are only accessible for a few moments until the feed loads, pushing the terms of service to the bottom of the screen again.

	• The text colour minimally contrasts the colour of the webpage background. As such, an additional standardized requirement could relate to the ease of access to terms of service. Ofcom may consider recommending that service providers make their terms of service accessible to users throughout their entire experience on the service. One way to achieve this would be to ensure that the terms of service are always "1 click away" from any given section on a service. For example, on the app version of the Instagram, the terms of service are "3 clicks" away from the user's main experience on the app. **48.** Yes, we agree with the including of 6AA in the Illegal Content Codes. It is reasonable expectation that service providers summarize the findings of their most recent children's risk assessments in their terms of service, or statement.
Recommender systems (Section 20)	
49. Do you agree with the proposed recommender systems measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 50. Are there any intervention points in the design of recommender systems that we have not considered here that could effectively prevent children from being recommended primary priority content and protect children from encountering priority and non-designated content?	Confidential? – NO **49.** Consistent with our previous responses throughout this consultation and our response to the Illegal Harms Consultation, we strongly believe that measures RS1-RS3 should not be limited to service providers that meet a certain level of risk or size. Given the risk of recommender systems across services likely to be accessed by children (which include small services) these measures should apply to **all** U2U services that operate a recommender system and are likely to be accessed by children. Similarly, children should be offered more control to allow them to indicate and provide feedback on certain types of content they do not wish to see, across **all** U2U systems. In other words, measures related to recommender systems should not be limited to only "large" services [RM3] and those at "medium or high risk for at least two kinds of PPC, PC, and the relevant kinds of NDC" for same reasons stated previously in this consultation.

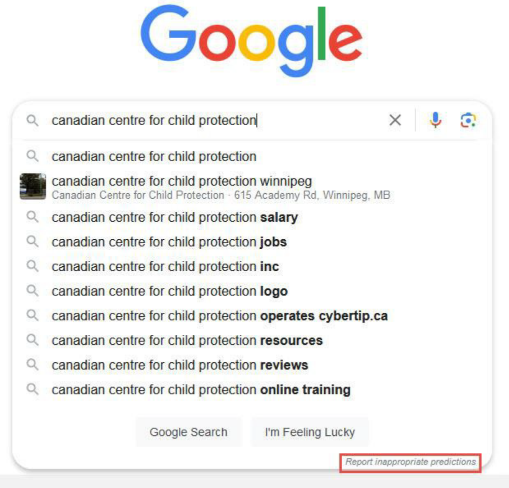
51. Is there any evidence that suggests recommender systems are a risk factor associated with bullying? If so, please provide this in response to Measures RS2 and RS3 proposed in this chapter. 52. We plan to include in our RS2 and RS3, that services limit the prominence of content that we are proposing to be classified as non-designated content (NDC), namely depressive content and body image content. This is subject to our consultation on the classification of these content categories as NDC. Do you agree with this proposal? Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3. • Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.	**Regarding paragraph 20.211:** W*e also do not consider it proportionate to recommend this* [RS3] *measure for smaller services,* ***even where they pose relevant risks****. In reaching this view we have considered that there are relatively high costs associated with implementing this measure in addition to the costs of Measures RS1 and/or RS2 which such services would be recommended to apply. Costs are uncertain and it is possible that some smaller services could incur costs above the lower end of our estimated rate. Also, while technically feasible, we understand that a personalised negative feedback loop can be complicated to implement, and so we are not confident that smaller services would be able to implement it with a reasonable level of cost in proportion to the benefits it would bring.* Small services that have any degree of relevant risk that should be expected to meet the obligations of these measures: Governments must normalize adherence to basic online safety standards, as an expected "cost of doing business" in the technology industry. We support safe innovation by companies of all sizes. In the same way that we establish, for example, clear and uniform food-handling rules for food establishments whether a small kiosk or a national fast-food chain, we hope that even small services have minimum requirements to ensure they protect and prevent children from exposure to harm. Regarding paragraph 20.207: "*These services are more likely to have both high numbers of children on the service*" As stated in our Illegal Harms Consultation response (questions 1, 3, and 8), size is not the determining factor for risk. Services aimed at children are likely to have smaller user bases. Platforms aimed at children can attract some adults who intend to harm children, but such platforms are intended for, and generally used by, a smaller portion of the population. **50.** Regarding paragraph 20.115 (b): Despite Meta's response to Ofcom's 2023 CFE ("*Meta told us that it adds a warning label to especially graphic or violent content so that it is not available to users under 18*") recent evidence that indicates users under the age of 18 are exposed to graphic content on Instagram: https://www.wsj.com/tech/instagram-recommends-

	sexual-videos-to-accounts-for-13-year-olds-tests-show-b6123c65 Ofcom may consider recommending that service providers make use of recommender systems that are specific to children (separate from those applied to adult users). As highlighted by the Wall Street Journal in June 2024 (referenced above), a 2022 internal analysis from Meta suggested that: *“The most effective way to prevent inappropriate content from being served to underage users would be to build an entirely separate recommendation system for teens”.* As to date, Meta has not implemented this recommendation. Regarding paragraph 20.47: Despite internal policies that govern recommendation systems, avoids “making recommendations that may be inappropriate for younger viewers”, underage users on Instagram are continuing to be exposed to harmful and age-inappropriate material as reported and tested by the Wall Street Journal (link above). While these measures are a good start for protecting children from harmful content and minimizing “rabbit holes” of this type of content, has Ofcom considered the harm for children caused by addictive algorithms, even when the content itself is not necessarily harmful? https://www.politico.eu/article/meta-hit-with-new-eu-probe-over-addictive-algorithms-harming-children/ **52**. Yes, we agree with this proposed inclusion. It is a reasonable expectation that service providers limit non-designated content (NDC) such as depressive content and body image content.
User support (Section 21)	
53. Do you agree with the proposed user support measures to be included in the Children’s Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence.	Confidential? – NO **53a**. For the same reasons stated throughout this consultation and our Illegal Harms consultation submission, measures US1-US3 should not be limited to U2U services that are “medium to high risk” for PC and PCC content. These measures reflect basic safety features, it must be ensured that children are provided with control over who they interact with and

b) If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.	what they see online, **even when the perceived risk of PC and PCC is low.** The application of US1-US3 across all U2U and search services likely to be accessed by children can still be applied in a manner that is proportional. Similar to our comments regarding measures related to content moderation, proportionality can still factor in but within the **degree** of user support provided. All relevant services should provide user support but the level of investment in these areas can be proportional to the need for support. Similarly measures US4-US6 should not be limited to only services that are large and multi-risk. Providing children with supportive information must occur across all services likely to be accessed by children, regardless of size and risk. **Paragraph 21.69** *Measure US2b: Global blocking of any non-connected account: U2U services should provide children with* ***a public user profile*** *a clear and accessible means of making themselves uncontactable to any user they do not have a mutually validated connection (that is, a connection that both users have agreed to)* How is a "public user profile" defined in this scenario? On Instagram, users can have private accounts (this is the default setting for users under 16). On private accounts, only "followers" or mutual connections) can view the private user's posts. **However, even when there is not a mutual connection, these private accounts are discoverable by other users on the platform**. Regarding the above scenario, Ofcom should consider extending measure US2b to private accounts held by children given their discoverability and the ability for unknown users to send connection and communication requests with private accounts. Because children with private accounts are still contactable by other users, extending US2b would ensure that children with private accounts are uncontactable. In a similar vein, children should be provided with the option of being uncontactable by other users, **even when there are mutual connections.** As detailed in our report "*An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion*", extorters often infiltrate a user's social network. With minimal

	effort, extorters can gain access to other users that are connected to their targets. Friends and followers lists provide extorters the opportunity to carefully curate their accounts by adding these friends and followers, giving them the appearance of a more authentic account by establishing mutual connections. Our research found that many victims of sextortion cited that the existence of mutual followers helped convince the victims that extorter accounts were legitimate. https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf **Paragraph 21.150:** *The current evidence does not support a single 'best practice' approach. It is for services to adapt, test and evaluate the effectiveness of the measure to their individual service.* ***We are not therefore proposing to make specific recommendations around how the information should be presented*** [US4]. At the very least, Ofcom may consider specific recommendations to standardize the presentation of material related to both US4 and US5. For example, it may be recommended that supportive information for child users should be displayed in a defined minimum font size. This is consistent with our statements regarding measures related to Terms of Service. **Paragraph: 21.191**: *This evidence suggests that both children and experts in children's mental health and wellbeing recognise the value of timely and appropriate signposting to support for children exposed to suicide, self-harm, eating disorder or bullying content.* ***There is less evidence for the effectiveness of signposting to support for exposure to other kinds of content harmful to children.*** We do not see a reason as to why this measure cannot and shouldn't be expanded to other types of content that is harmful to children, including violent, drug-related, and pornographic content. Additional intervention points for Ofcom to consider regarding measure US5: • When children engage with harmful content, including commenting, liking, saving, or sharing this type of content.

	The current intervention points (2 and 3) require a high degree of engagement with harmful material.
Search features, functionalities and user support (Section 22)	
54. Do you agree with our proposals? Please provide underlying arguments and evidence to support your views. 55. Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour? 56. Are there additional steps that you take to protect children from harms as set out in the Act? a) If so, how effective are they? As referenced in the Overview of Codes, Section 13 and Section 17, the use of GenAI to facilitate search is an emerging development and there is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this section. We welcome further evidence from stakeholders on the following questions and please provide arguments and evidence to support your views: 57. Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? Please provide arguments and evidence to support your views.	Confidential? – NO **54**. Yes, these proposals are a good starting point for ensuring that children and adult users are empowered to report harmful content and children are provided with resources when potentially encountering harmful content. However, consistent with the notion that all services should be required to meet basic safety obligations, SD1 and SD2 should be extended to all general search services, regardless of size. As stated in our submission to the Illegal harms Consultation (specifically question 3), services, including search services, aimed at children are likely to have smaller user bases. Platforms aimed at children are intended for, and generally used by, a smaller portion of the population. Such services are less likely to meet a user threshold that is based on the entire population, and a more appropriate measure would be the number of child users. Regarding paragraph **22.39**: "*To effectively reduce reporting barriers, we propose that reporting tools should be easy to find and easily accessible in relation to the predictive search suggestions themselves*." Ofcom may seek to clarify **where and when** the reporting option is made available to users. It should be required that users do not have to carry out the search containing the harmful suggestion as a prerequisite to reporting that search suggestion. In other words, users must be provided the tools to report harmful search suggestions without having the carry out the search. As highlighted by Ofcom in paragraph 22.39, Google currently provides a reporting option, however it is nondescript. This is due to the location of the text,

	the font size, and colour (e.g. lack of contrast):  canadian centre for child protection canadian centre for child protection canadian centre for child protection winnipeg Canadian Centre for Child Protection · 615 Academy Rd, Winnipeg, MB canadian centre for child protection **salary** canadian centre for child protection **jobs** canadian centre for child protection **inc** canadian centre for child protection **logo** canadian centre for child protection **operates cybertip.ca** canadian centre for child protection **resources** canadian centre for child protection **reviews** canadian centre for child protection **online training** Google Search I'm Feeling Lucky *Report inappropriate predictions* Given the example highlighted above, Ofcom may consider a standardized approach in their recommendations on how services display these reporting options: this could include a defined minimum font size and colour to ensure these tools are easily accessible to users. **55**.See our response to question 19(i) in our submission to the Illegal Harms consultation.

Combined Impact Assessment (Section 23)	
58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?	Confidential? – Y / N **58.** As we've stated, the assessment of whether a service is "likely to be accessed by children" is critical and must be done in a way that scopes in services that present a risk to even a few children. In our view, every service should be required to have basic safety, governance and accountability measures to help keep children safe online. We recognize that under the Online Safey Act, the duties regarding child's risk assessments and protecting children's online safety apply to services that are "likely to be accessed by children". We believe that it is fundamentally flawed to permit certain services to have zero child-safety measures, and this may leave gaps that those seeking to harm children exploit. 23.11 CONSULTATION 2 - CHILD PROTECTION CONTRADICTION, GA2 as an example, is it **ALL LIKELY TO BE ACCESSED** or is it **ALL**? VOLUME 4 – **Measure GA2: Accountable person ... 11.55** We propose that providers of all user-to-user and search services **likely to be accessed by children should implement this measure**. **11.56** The service provider should name a person accountable to its most senior governance body for compliance with the children's safety duties for services likely to be accessed by children. https://www.ofcom.org.uk/__data/assets/pdf_file/0031/284485/vol4-assessing-risks-of-harms-to-children-online.pdf VOLUME 5 - Proposed core measures recommended for all services......23.14 The core measures below are recommended for **all services, regardless of size, risk or any other criteria**. This would therefore include low-risk services provided by small and micro businesses, among others.......**GA2 Name a person accountable to most senior governance body for**

	compliance with children's safety duties. REFERENCE TABLE23.1 https://www.ofcom.org.uk/__data/assets/pdf_file/0032/284486/vol5-what-should-services-do-to-mitigate-risks.pdf CONSULTATION 1 – ILLEGAL HARMS VOLUME 3 ... pg. 5 .....8. Governance and accountability https://www.ofcom.org.uk/__data/assets/pdf_file/0021/271146/volume-3-illegal-harms-consultation.pdf **We are making the following proposals for all services**: - Name a person accountable to the most senior governance body for compliance with illegal content duties and reporting and complaints duties. **We are making the following proposals for all multi risk services** and all large services: - Written statements of responsibilities for senior members of staff who make decisions related to the management of online safety risks. - Track evidence of new kinds of illegal content on their services, and unusual increases in particular kinds of illegal content, and report this evidence through the relevant governance channels. U2U services should also track and report equivalent changes in the use of the service for the commission or facilitation of priority offences. - A Code of Conduct that sets standards and expectations for employees around protecting users from risks of illegal harm. - That staff involved in the design and operational management of the service are sufficiently trained in the service's approach to compliance." VOLUME 4 - **Protecting people from illegal harms online** https://www.ofcom.org.uk/__data/assets/pdf_file/0022/271147/volume-4-illegal-harms-consultation.pdf Pg. 4. "We propose to define a service as multi-risk where it is high or medium risk for at least two kinds of illegal harms."

	~~ NOTE C3P RESPONSE TO CONSULTATION 1 “We firmly support minimum requirements and basic obligations for ALL services, and are pleased to see that all services must name someone responsible for compliance with illegal content duties and reporting and compliance duties (Chapter 8), and all U2U and search services have certain requirements in Chapter 9 of Volume 3. A key theme in our remaining responses will be the notion that the concept of basing child safety proportionally on the popularity of a product does not exist in the physical world, and should not exist online. Services should be scoped in based on risk and functionality, not size.”
Statutory tests (Section 24)	
59. Do you agree that our proposals, in particular our proposed recommendations for the draft Children’s Safety Codes, are appropriate in the light of the matters to which we must have regard? a) If not, please explain why.	Confidential? – NO **We disagree with the broad application of “likely to be accessed by children” as an exemption to participating in basic Children Safety practices**. Focusing on core Governance and Accountability measures and recognizing the flexibility (i.e. proportionate / scalability) that has been introduced throughout these consultations GA1 – GA7 should be required for ALL services not just those that determine a likelihood of being accessed by children. The reality is that any service can likely be accessed by a child, case in point would be services like known pornography and gambling sites which are by legal definition adult only. Studies show it is not uncommon for children to access pornography on online (e.g. https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.250), and not uncommon to access gambling online (e.g. https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2019), if these highly controlled activities are accessed by children it is safe to assume any site is likely to be accessed by a child. For these reasons Ofcom is strongly encouraged to apply the “likely to

	be accessed by children” broadly to any service that is considered part the regulation as a Search service or User-to-user service.
Annexes **Impact Assessments (Annex A14)**	
60. In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? 61. In relation to our Welsh language assessment, do you agree that our proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English? a) If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	Confidential? – Y / N

Please complete this form in full and return to protectingchildren@ofcom.org.uk.