Question (Volume 2)	Your response
	Children all over the world are exploited in this manner. See Brazil case, “Brazil: Two arrested in global hunt to catch child predators.” 14 April 2021, See Romania case, “Sask. Appeal Court increases sentence for child pornographer Philip Chicoine – Saskatoon.” 17 October 2019. See Thailand case, “Man pleads guilty to seeking violent sex abuse images from source in Thailand.” 24 July 2023. Section 6.13 accurately notes that livestreaming is a risk factor for several kinds of illegal harm, including the livestreamed child sexual abuse of Filipino children, often at the direction of paying offenders in the UK. In IJM's experience partnering with the Philippine government to safeguard over 1,200 individuals in the Philippines from online sexual exploitation and support nearly 400 suspected trafficker arrests, we have seen that this crime is pervasive, prevalent on the surface web and thrives in end-to-end encryption (E2EE). According to ECPAT France, “The child sex offenders who are willing or prefer to pay in order to participate in live online child sexual abuse consider it less risky because there is more distance with child victims. Additionally, it requires less efforts than soliciting children for sexual purposes and there are less chances that child victims report the sexual abuse. As a result, they rather get involved in live online child sexual abuse which results for the trafficking of children.” Additionally, the lack of safety technology is a potential cause of online harms. The ease with which predators and sex offenders can create, distribute, and produce child sexual exploitation material is a risk factor for any service that does not deploy prevention technology. In IJM's collaborative casework model in partnership with the Philippine government, offender impunity is a driving factor for individuals willing to abuse children via livestream. The University of Edinburgh's Childlight recently found that “"Men in Australia, UK and USA who report online sexual offending behaviours against children also report being 2-3 times more likely to seek sexual contact with children between the ages of 10-12 years old if they were certain no one would find out."

Question (Volume 2)	Your response
	An additional high-risk flag given the known link between the UK (as the second top consumer of online sexual exploitation and abuse of children in the Philippines) and Philippines of livestreamed child sexual abuse would include profiles posting or sharing illicit content or using illicit keywords when the accounts are from the UK and Philippines respectively. Companies that operate in both countries and allow for child sexual abuse material to be livestreamed between these two countries should be marked as high-risk. Finally, the lack of quality reports to law enforcement should be deemed a risk factor to platforms. The lack of quality reports issued by tech companies to NCMEC that are then routed to national law enforcement mean that offenders are unlikely to be found. In IJM's experience supporting Kenyan, Nigerian, Ghanaian, Filipino, and Malaysian law enforcement to investigate the reports created by the tech sector, reports to law enforcement far outpace the capacity of law enforcement to respond to them. If tech companies include more information in these reports, law enforcement can conduct these investigations more quickly and address more cases. If the mandatory reporting by tech platforms of suspected CSAM included the IP address and PORT information, these reports would likely be more actionable. The US REPORT Act that is currently under review with the Senate is an excellent example of potential legislation that would strengthen law enforcement reports and improve their capacity to investigate suspected child sexual abuse and ultimately hold perpetrators accountable.
Question 6.2: Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	IJM commends the identification of several risk factors for several types of illegal harms, particularly the platform functional risks such as messaging capabilities, end-to-end encryption, livestreaming functionalities, easy-to-sign-up services, and less-popular platforms being easy targets for offenders. It also important that the U2U user-base definition does not have to include registered users. One of the significant challenges highlighted is the vulnerability of victims of online sexual exploitation in the Philippines who

Question (Volume 2)	Your response
	may not be direct users of the platforms where the exploitation occurs. Rather, it often involves the use of adult accounts controlled by traffickers in the Philippines who establish connections with remote offenders, often residing in western countries like the UK. Recognizing this dynamic underscores the importance of considering the platform risk factor, where children need not be users themselves to fall victim to exploitation. Additionally, an alarming unidentified risk factor is the lack of adequate safety technology implementation to prevent the capture of CSAM. The absence of safety measures such as SafeToWatch or other client-side scanning image-classifiers for detecting new CSAM poses a serious threat to the safety and well-being of potential victims. There is an urgent need for platforms and service providers to adopt advanced technological solutions that proactively identify and mitigate the dissemination of harmful content, ensuring a safer online environment for users, particularly vulnerable individuals at risk of exploitation. The 2023 WeProtect Global Alliance Global Threat Assessment outlines several technological alternatives for deployment that can prevent, disrupt, and detect CSAM: "Client-side scanning, which involves scanning messages on devices for matches or similarities to a database of illegal child sexual abuse material before the message is encrypted and sent). Homomorphic encryption. This is the use of a different type of encryption which allows operations to be performed without data decryption at any point). Intermediate secure enclaves, which decrypt the message at server level by a third party and use tools to detect child sexual abuse materials." Some technology companies allow for the viewing of CSAM, even if the tech platform has identified it as CSAM by including the option to 'see results anyway.' This function should be deemed high-risk, as it presents a concerning feature that enables offenders to click and view potentially harmful content, including CSAM. The inclusion of such a feature emphasizes the need for stringent measures to mitigate the associated risks with these platform functionalities that could potentially facilitate the spread of CSAM.

Question (Volume 2)	Your response
	[✂] Lack of signal sharing by tech platforms of livestreamed abuse is a key gap to identify and block child sexual abuse offenders. “The Tech Coalition is launching Lantern, the first cross-platform signal sharing program for companies to strengthen how they enforce their child safety policies. Online child sexual exploitation and abuse (OCSEA) are pervasive threats that can cross various platforms and services. Two of the most pressing dangers today are inappropriate sexualized contact with a child, referred to as online grooming, and financial sextortion of young people. To carry out this abuse, predators often first connect with young people on public forums, posing as peers or friendly new connections. They then direct their victims to private chats and different platforms to solicit and share child sexual abuse material (CSAM) or coerce payments by threatening to share intimate images with others." Finally, the overemphasis of detecting known CSAM and deprioritizing the detection of new CSAM including livestreaming has the potential to incentivize the new production of CSAM by offenders, given that companies are least likely to detect and report it. In other words, children are put in harm's way to create new content because offenders may deem sharing known content to be riskier.

Question (Volume 3)	Your response
Question 8.1: Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.	The governance and accountability measures in the illegal content Codes of Practice put forth by Ofcom are a good start. However, the Organisation for Economic Co-operation and Development examined the top-50 online platforms' transparency reporting and their policies and procedures in relation to CSEA. 80% of the platforms provided no detailed policy on OSEAC, 60% of the platforms did not issue a transparency report on CSEA, and information in transparency reports was found to be inconsistent and uneven, making sector-wide analysis difficult, if not impossible. This study demonstrates the need for global collaboration and cross-governmental unity in transparency reporting, particularly on part of the respective regulatory bodies. Further developing the overseas regulatory network and aligning with other governments to create cohesive transparency reporting will i) give deeper insights into online sexual exploitation and ii) allow experts to develop a cohesive global response to this crime across tech platforms and geographic boundary lines. Australia is already seeking to do this with the review of their Online Safety Act. Additionally, the implementation of protection measures should be measured and tracked. Australian eSafety Commissioner has powers to require one-off and periodic reporting as it relates to the implementation of safety measures. Consider the following questions in transparency reporting: 1) How much (and what percentage of your annual profit?) did your company spend on online safety this month (or annually?) in proportion to its profits? 2) What is the status of implementing grooming, livestreaming, and known CSAM detection and prevention technologies? 3) What is the average response time to reports of child sexual exploitation and abuse?

Question (Volume 3)	Your response
Question 8.2: Do you agree with the types of services that we propose the governance and accountability measures should apply to?	
Question 8.3: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?	
Question: 8.4: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?	
Question 9.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 9.2: Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?	

Question (Volume 3)	Your response
Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?[1]	
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	
Question 10.2: Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?	

[1] If you have comments or input related the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

Question (Volume 4)	Your response
Question 11.1: Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?	
Question 11.2: Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?	*[Is this answer confidential? Yes / No (delete as appropriate)]* Chapter 6 of the codes demonstrates the potential and likely strategies employed by offenders who may exploit less developed or smaller online services to evade detection, as these platforms are less likely to deploy robust CSAM detection or prevention technologies. Consequently, it is imperative that even smaller or seemingly less risky companies adhere to every measure outlined in the Codes, ensuring an indiscriminate application of safety protocols. Given the diverse range of platforms available for offenders to exploit children on, coupled with their increasing creativity in conducting that exploitation, it becomes crucial for companies to adopt comprehensive prevention measures. Companies should prioritise building platforms that are safe by design, making it a baseline expectation for all, rather than a concern limited to perceived 'risky' entities. This analogy is akin to ensuring all cars, not just high-performance ones or those manufactured by the largest automakers, are equipped with safety measures, emphasising the universal need for a maximum level of prevention across the digital landscape. We expect all auto manufacturers to apply the same emissions and safety standards, all car seat companies to apply the same rigorous protection technology, and all infant crib designers to perform required safety checks. It's time we apply the same standards to the tech companies. There have also been more recent instances of sextortion offenders meeting children on larger platforms but moving to smaller ones to continue the exploitation. As part of the extortion and account takeover, they take over the child's school account end extort all of the other children within the platform. It's a cross platform issue that smart offenders are using to get into the child's closer network. This has been seen specifically in school communication

Question (Volume 4)	Your response
	platforms. Smaller platforms are not exempt from being used to abuse children.
Question 11.3: Do you agree with our definition of large services?	The designation of 7 million users amounts to approximately 9.6% of the British population. Comparatively, Australia's Industry Codes impose their most stringent sections on providers with a minimum threshold of 2.5% of the population as monthly active users. It is recommended that Ofcom consider aligning with this criterion to encompass smaller or less-used UK services that may facilitate online harm to children across borders. None of the requirements imposed on larger services should be seen as luxuries specific to services with a large enough business. Complying with safety technology should be a basic requirement for online services, similar to paying for security or their internet bill. Online safety is not a luxury but is instead a necessity for any tech company looking to start its business in the UK. Services used by a small percentage of the UK population might be a niche service used primarily by offenders. By inadvertently excluding smaller services from specific requirements of the Online Safety Act, offenders could be enabled to use smaller companies to exploit children where no one is looking. Finally, Volume 4 comments that smaller platforms may not have capacity to deploy certain technological solutions to due lack of financial resourcing. However, many of the technologies are available free of charge or for low cost. For example, the following tools are available for no cost: • Microsoft’s PhotoDNA • NCMEC’s Hash Sharing • Google Content Safety API and CSAI Other tools are available for low cost. For example, the monthly cost of DragonflAI, for 500,000 active users is approximately £1200.12. For Thorn’s Safer tool, a 12-month subscription based on 1M queries per month is $30,720 USD.

Question (Volume 4)	Your response
Question 11.4: Do you agree with our definition of multi-risk services?	*[Is this answer confidential? Yes / No (delete as appropriate)]* Chapter 6 of the codes demonstrates the potential and likely strategies employed by offenders who may exploit less developed or smaller online services to evade detection, as these platforms are less likely to deploy robust CSAM detection or prevention technologies. Consequently, it is imperative that even smaller or seemingly less risky companies adhere to every measure outlined in the Codes, ensuring an indiscriminate application of safety protocols. Given the diverse range of platforms available for offenders to exploit children on, coupled with their increasing creativity in conducting that exploitation, it becomes crucial for companies to adopt comprehensive prevention measures. While the definition of multi-risk is understandable, multi-risk services should have the same responsibilities as those perceivably less risky. There have also been more recent instances of sextortion offenders meeting children on larger platforms but moving to smaller ones to continue the exploitation. As part of the extortion and account takeover, they take over the child's school account end extort all of the other children within the platform. It's a cross platform issue that smart offenders are using to get into the child's closer network. This has been seen specifically in school communication platforms. Even services that would assumably be less risky should have deploy safety technology to prevent child exploitation.
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[2]	The Codes of Practice outlined in Annex 7 consist of several key features toward building a safer internet, such as systems that take down illegal content (4A). This is imperative to stop the dissemination of CSAM which revictimizes children each time it is shared. **Technological Feasibility** 4G of the Codes indicates that platforms are only responsible for implementing perceptual hash matching technologically if it is feasible. However, Australian eSafety Commissioner has paved a road in its partnership with Industry

[2] See Annexes 7 and 8.

Question (Volume 4)	Your response
	to develop the DIS (Designated Internet Services) and RES (Relevant Electronic Services) codes which include a requirement for providers to invest resources into making it technologically feasible for their platforms to implement safety technology. IJM recommends that Ofcom adopt a similar measure and require technology companies to invest in and build their platforms safely. Similarly, this applies to URL detection technology in section 4H and search services in Annex 8. Providers should be investing in technology that detects and prevents uploading, sharing, or generating CSAM URLs. The additional comparison to be made is that eSafety sets a timeline for which safety tech should be implemented for both known and new CSAM, and this should be mirrored in the UK. Safety technology developed by Microsoft, Google, and others has been a collective approach to child safety. This is not a competitive space. Tech companies can and should work together, pooling their collective resources to collaboratively design innovative solutions that address the existing CSAM crisis. **Trusted Flaggers** Section 5I of Annex 7 indicates a list of trusted flaggers of illegal content, but in this list excludes Police Scotland, Police of Northern Ireland, North Wales Police, and South Wales Police. In just one example, Police Scotland is heavily involved in identifying and apprehending offenders. Consider expanding Trusted Flagger status to all relevant law enforcement agencies. Gary Campbell admitted 13 charges of sexual assault causing Filipino children to become providers of sexual services and rape while Campbell directed the livestreamed abuse. This case was supported by Police Scotland. CyberSafe Scotland, an organisation based in Aberdeen focused on empowering, educating, and protecting children online. One of their key partners is Police Scotland. Because Police Scotland is heavily involved in investigating and supporting cases of child sexual abuse online, IJM highly recommends that each national police agency is included in the trusted flagger program.

Question (Volume 4)	Your response
	Additionally, INHOPE outlines that 'Under the Digital Services Act (DSA), Trusted Flagger are defined and organisations operating within the EU have obligations to cooperate with recognised Trusted Flaggers which include EU based hotlines in many countries.' Consider expanding the Trusted Flagger program beyond law enforcement to civil society, NGOs, and SMEs with appropriate training.
Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?	Many of the technologies are available free of charge or for low cost. For example, the following tools are available for no cost: • Microsoft's PhotoDNA • NCMEC's Hash Sharing • Google Content Safety API and CSAI Other tools are available for low cost. For example, the monthly cost of DragonflAI, for 500,000 active users is approximately £1200. For Thorn's Safer tool, a 12-month subscription based on 1M queries per month is $30,720 USD. Because some tools, such as SafeToWatch (HarmBlock) do not lead to the creation of reports but simply disrupt illegal or harmful content from ever reaching the platforms' servers, implementing such technologies would imply less need for content moderators, thus reducing costs for the company overall while safeguarding children across the globe. IJM's experience partnering with the Philippine government to combat online sexual exploitation of children has found that a majority of the abuse taking place includes contact offending on part of the trafficker or other children. Regardless of whether an individual in the UK is physically abusing a child, a child is being physically abused in person because of the demand created by the offender based in the UK. Therefore, we must treat this issue with the same severity and urgency as contact offending. According to the recent study conducted by Childlight, the University of Edinburgh's research institute on CSA, "Men in Australia, UK and USA who report online sexual offending behaviours against children also report being 2-3 times more likely to seek sexual contact with children between

Question (Volume 4)	Your response
	the ages of 10-12 years old if they were certain no one would find out." Furthermore, Australia's Institute of Criminology assessed the link between livestreaming child sexual abuse and contact offending. The study found that four out of seven offenders travelled to sexually abuse a child in person either before or after having viewed livestreamed child sexual abuse. These studies and IJM's casework experience demonstrate that online sexual exploitation of children has a direct correlation to contact offending. It is imperative that both Ofcom and tech companies apply safety technology and prevention measures to deter criminals on par with contact offending. Ofcom must also consider the costs associated with parents going to jail, both from the societal cost of housing prisoners and the cost to a family of missing a parent. The Guardian reports that hundreds of homes are visited by police officers each month because someone in the home is viewing images of child abuse. This visit is often referred to as 'The knock.' Lucy Faithful Foundation says police are addressing more than 900 suspected CSAM offenders each month. With detection and prevention technology, British children can still have their parents and half a million Filipino children will never have their abuse livestreamed to a foreign offender again. The Guardian also recently shared about the uptick in underage CSAM offenders. There is a massive cost to society for underage CSAM offenders – some of whom are finding this material by accident and become addicted to it – consuming more and more violent material.
Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	In section 12.110 under prioritisation of content, 'privately' sent content should be included as a top priority for internal review given the frequency with which private communications are used to exploit or extort children. In IJM's partnership with the Philippine government to safeguard over 1,200 children and conduct over 360 operations, we have continued to see a majority of child sexual abuse creation, production, and dissemination via private channels such as through direct messaging and video conferencing. An additional high-risk flag given the known link

Question (Volume 4)	Your response
	between the UK (as the second top consumer of online sexual exploitation and abuse of children in the Philippines) and Philippines of livestreamed child sexual abuse would include profiles posting or sharing illicit content or using illicit keywords when the accounts are from the UK and Philippines respectively. For further details on key indicators of livestreamed child sexual exploitation that can help with aligning prioritisation efforts of tech, please review the second document in this consultation (attached).
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 14.1: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.	**Technological Proposals** IJM encourages Ofcom to go a step further from the three proposals for technological support for content moderators. Going beyond hash matching and URL detection, require tech companies deploy image-classifiers, machine learning, and AI. These types of technologies are not only recommended by WeProtect Global Alliance, but are also currently in use on many major platforms. It is entirely possible to assess, and remove material, even in an encrypted environment: 1. Apple created a technology using **client-side hashing** called NeuralHash that ensures privacy for both end-users and survivors of child sexual abuse and exploitation. As explained by Dr. Hany Farid, client-side hashing technology extracts and encrypts the hash from the sender, decrypts the hash at the server level, and only sends on non-CSAM content. 2. Similarly, technology exists whereby **secure enclaves** within company servers decrypt a message, compute a hash, and block CSAM from being sent beyond the server. This type of detection technology is hosted at the service provider but is not visible by anyone at the company.

Question (Volume 4)	Your response
	Client-side hashing technology is currently already being used by end-to-end encrypted service providers. For example, WhatsApp detects harmful content such as 'suspicious links' through scanning text messages and flagging them. As described on the company's website, *"WhatsApp automatically performs checks to determine if a link is suspicious. To protect your privacy, these checks take place entirely on your device, and because of end-to-end encryption, WhatsApp can't see the content of your messages."* This detection and scanning technology maintains legally protected user privacy rights (it does not "break" encryption) while still protecting end-users from malware. **Similar technology can be used to detect CSAM and protect vulnerable children, while also keeping illegal and harmful content off of platforms.** **Content Prioritisation** A majority of child sexual abuse creation, production, and dissemination via private channels such as through direct messaging and video conferencing. An additional high-risk flag given the known link between the UK (as the second top consumer of online sexual exploitation and abuse of children in the Philippines) and Philippines of livestreamed child sexual abuse would include profiles posting or sharing illicit content or using illicit keywords when the accounts are from the UK and Philippines respectively.
Question 14.2: Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?	The guidance issued is slightly unclear as it relates to 'privately' or 'publicly' communicated content. In general, nearly all content is easily shareable because someone can take a screenshot or record their screen via software or a secondary device. Further clarity is needed to define these terms.
Question 14.3: Do you have any relevant evidence on: • The accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;	PhotoDNA is a perceptual hash matching technology that is entirely free for use. According to renowned professor Dr. Hany Farid of University of California Berkley in his US Congressional testimony, "the robust image hashing technique used by PhotoDNA has an expected error rate of approximately 1 in 50 billion." Additionally, NCMEC's Hash Sharing and Google's Content Safety API and CSAI are free

Question (Volume 4)	Your response
- The ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers; - The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching[3] for CSAM URL detection; - The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and - An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.	of charge. Consider the accuracy of these tools which afford a massive amount of protections to victims of CSA. A fractional amount of inaccuracy is worth ensuring children are not sexually abused, and there many ways to minimize the consequences of inaccuracies. Other tools are available for low cost. For example, the monthly cost of DragonflAI, for 500,000 active users is approximately £1200. For Thorn's Safer tool, a 12-month subscription based on 1M queries per month is $30,720 USD. IWF's Hash List is available as part of their membership program which has scaled pricing depending on company size.
Question 15.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*

[3] Fuzzy matching can allow a match between U2U content and a URL list, despite the text not being exactly the same.

Question (Volume 4)	Your response
Question 16.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 17.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 17.2: Do you have any evidence, in particular on the use of prompts, to guide further work in this area?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 18.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 18.2: Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 18.3: Are there other points within the user journey where under 18s should be informed of the risk of illegal content?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
Question 19.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 19.2: What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 19.3: We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive. Are you aware of any other design parameters and choices that are proven to improve user safety?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 20.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
Question 20.2: Do you think the first two proposed measures should include requirements for how these controls are made known to users?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 20.3: Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 21.2: Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically: • What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)? What are the advantages and disadvantages of the different options, including any potential impact on other users?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
• How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed? • There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users. What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?	
Question 22.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 23.1: Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 23.2: Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
for whom we propose to recommend more measures?	
Question 23.3: We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 24.1: Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard? If not, why not?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 5)	Your response
Question 26.1: Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 26.2: Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 5)	Your response
Question 26.3: What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 6)	Your response
Question 28.1: Do you have any comments on our proposed approach to information gathering powers under the Act?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Annex 13)	Your response
Question A13.1: Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Annex 13)	Your response
Question A13.2: 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.	*[Is this answer confidential? Yes / No (delete as appropriate)]*

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

Annex A: Livestreamed Child Sexual Abuse and New Production Cases

‘DREADFUL’ DEVON CHILD ABUSER JAILED FOR 18 YEARS

UK-based offender paid Filipino facilitators and directed them via Skype as he watched and recorded 102 hours of livestreamed sexual abuse of up to 46 child victims.

QUEENS MAN SENTENCED TO 15 YEARS’ IMPRISONMENT FOR PRODUCING CHILD PORNOGRAPHY

In two months, US-based offender paid and directed Filipino facilitators to engage in sexual acts with children and reordered over 50 video conferences depicting the abuse, some livestreamed via Skype.

PAEDOPHILE, 74, DIRECTED CHILD ABUSE FILMS ON SKYPE 7,000 MILES AWAY FROM HIS HOME

Over a 3-year period, UK-based offender paid 8 facilitators to carry out sex acts and livestream the abuse of female children (aged 6 and 9) in the Philippines via Skype.

FIVE YEARS IN JAIL AND WORLDWIDE TRAVEL BAN FOR BRITISH TEACHER WHO WANTED TO ABUSE YOUNG FILIPINO CHILDREN

UK-based offender sent at least 15 wire transfers to adult facilitators in the Philippines for images and livestreamed videos of children being sexually exploited; in addition, he attempted to arrange travel to the Philippines over Skype conversations.

EX-BRITISH ARMY OFFICER JAILED FOR ONLINE CHILD SEX ABUSE IN PHL

Over a 2-year period, UK-based offender made nearly 50 payments to direct and view livestreamed child sexual exploitation material (CSEM) of multiple Filipino children via Skype.

CONVICTED CHILD SEX OFFENDER BEHIND BARS AGAIN FOR ILLICIT SKYPE RELATIONSHIP WITH FILIPINO CHILDREN UNDER 12

Over a 4-and-a-half-year period, Australia-based offender paid a Filipino family over $26,000 for continued livestreamed CSEM of two sisters (age 2 and 7 when the abuse began) via Skype.

MAN GETS 30 YEARS FOR MAKING CHILD PORN USING KIDS IN PHL

US-based offender directed Filipino facilitators to perform sexual acts on children (infants to age 10) while he watched via Skype, in exchange for money.

PAEDOPHILE WHO PAID FILIPINO MUMS FOR PICTURES OF NAKED DAUGHTERS IS JAILED

Over a 3-year period, UK-based offender communicated with facilitators in the Philippines via Skype and provided 36 payments for CSEM of girls aged 5 to 12 years old.

KANSAS MAN SENTENCED FOR PRODUCING CHILD PORNOGRAPHY

US-based offender travelled to the Philippines to film himself engaging in sex act with minor females as well as communicating via Skype with a child's mother and directing her to livestream CSEM depicting an 8-year-old female.

BUSINESSMAN ADMITS PAYING FOR ONLINE CHILD ABUSE FROM PHILIPPINES

Over a 2-year period, UK-based offender directed an adult facilitator for livestreamed abuse of Filipino children (as young as 10 years old) via Skype, in exchange for over £5,500.

SHELBY COUNTY MAN SENTENCED TO 27 YEARS IN PRISON FOR SENDING MONEY TO FILIPINO MOTHERS IN EXCHANGE FOR CHILD PORNOGRAPHY

Over a 3-month period, US-based offender directed Filipino facilitators over Skype to share sexual images and videos of their children in exchange for payments via MoneyGram.

JAIL FOR MAN WHO EXPLOITED GIRLS IN THE PHILIPPINES

Australia-based offender directed 13-year-old Filipina girl over Skype to undress and perform lewd acts in exchange for money.

VILE SEX PREDATOR PAID POOR FAMILIES IN THE PHILIPPINES TO ABUSE THEIR OWN CHILDREN AS YOUNG AS THREE AS HE WATCHED ON SKYPE

Australia-based offender directed adult Filipina women over Skype to perform sexual acts on children in exchange for money; he had at least 13 victims aged between three and nine years old who were abused on 74 occasions.

FORMER RTÉ PRODUCER FILMED HIMSELF SEXUALLY ABUSING A GIRL IN THE PHILIPPINES

Among multiple child exploitation offenses, Ireland-based offender paid an adult facilitator in the Philippines to send him CSEM depicting a 13-year-old girl over Skype.

MAN PAID $40 TO WATCH FILIPINO CHILD ABUSE

On multiple occasions, Australia-based offender used Skype to direct livestreamed shows of girls under 16 in the Philippines in exchange for money.

BRITISH PENSIONER, 68, IS JAILED FOR 12 YEARS AFTER PAYING £3,000 TO MOTHER IN THE PHILIPPINES TO RECEIVE SEXUAL ABUSE IMAGES OF HER SIX-YEAR-OLD CHILD

UK-based offender admitted to 67 separate offences, including using Skype to contact the mother of the child in the Philippines and making online payments in order to facilitate the sexual exploitation of the child victim and sending images of the abuse.

WINNIPEG MAN WANTED IN PHILIPPINES FOR ALLEGEDLY PAYING TO WATCH CHILD SEX ABUSE

Canada-based offender is wanted for wiring thousands of dollars to facilitators in the Philippines for child exploitation offenses including livestreaming the sexual abuse of children via Skype.

EX-DJ MARK PAGE 'ARRANGED SEX WITH PHILIPPINE CHILDREN

UK-based offender is charged with multiple child exploitation offenses that occurred from 2016 – 2019, including directing Filipino children to perform sexual acts over Skype in exchange for money.

NYC 'ORIGINAL GEEK' IN CHILD PORN CASE TARGETED KIDS VIA INSTAGRAM, SKYPE: FEDS

Over a 4-year period, US-based offender engaged in sexually explicit Skype communications with at least eight underage victims, in the U.S. and abroad, between the ages of 13 and 17. He was charged with producing child pornography after prosecutors alleged, he directed children to send him sexually explicit images and videos after targeting them via Skype.

BEAUFORT COUNTY MAN SENTENCED TO 30 YEARS FOR PRODUCTION OF CHILD PORNOGRAPHY

US-based offender admitted to assaulting a 22-month-old victim approximately five times between September 2019 and December 2019, and live streaming these assaults over Skype to an offender in the UK.

MAROUBRA MAN PLEADS GUILTY TO CHILD ABUSE, GROOMING CHARGES

Australian-based offender pleaded guilty to procuring a child under 16 for unlawful sexual activity and possessing and transmitting child abuse material, after using Skype to groom and approach the victim.

TWISTED PAEDO 'USED FORNITE & CALL OF DUTY TO PREY ON KIDS & FORCE THEM TO POSE NAKED AS COPS FIND 2,000 ABUSE IMAGES'

Previously convicted Spain-based offender made 81 payments to at least 26 victims between the ages of eight and twelve using online gaming platforms, then convinced them to appear naked on Skype.

THE FALL OF A SERIAL SEXTORTIONIST

Mexican-based offender was sentenced to 34 years in prison for the production of child pornography after using multiple social media platforms, including Skype, in a sextortion scheme that victimized more than 100 girls and women around the world.

LAS VEGAS MAN SENTENCED TO 12 YEARS IN PRISON FOR DISTRIBUTION OF CHILD SEXUAL ABUSE MATERIAL

US-based offender was sentenced to 12 years in prison for distributing images of CSAM after Skype reported his account to the National Center for Missing and Exploited Children regarding the upload of files containing CSAM.

ST. PAUL MAN SENTENCED TO 43 YEARS IN PRISON FOR TARGETING MORE THAN 1,100 MINOR VICTIMS IN SEXTORTION SCHEME

Over a period of several years, US-based offender victimized more than 1,000 young girls through a sextortion scheme that utilized multiple social media platforms, including Skype.

COMMUNITY SERVICE FOR CHILD ABUSE FANTASY

Australian-based offender pleaded guilty to one count of making or reproducing child exploitation material after using Skype to fantasize about the sexual abuse of a young girl in “disturbing and graphic detail.”

AYDIN COBAN SENTENCED TO 13 YEARS FOR SEXUAL EXTORTION OF AMANDA TODD

Netherlands-based offender was sentenced to 13 years for extortion, two counts of possession of child pornography, child luring and criminal harassment after using multiple social media platforms, including Skype, to demand web shows from a teenage girl over a period of 3 years until she died by suicide.

Norfolk man jailed for child sex offences in the Philippines

06/10/2023 - A man 'stage managed' the sexual abuse of children in the Philippines by paying for videos of them, having described in "graphic and disgusting" detail what he wanted to happen to them. Hockley, of Canterbury Way, Thetford, appeared at court for sentencing having been previously found guilty of arranging or facilitating child prostitution or pornography in that he intentionally arranged the sexual exploitation of children between May 1, 2015, and January 22, 2017. He was also found guilty of three counts of making indecent photographs of children on or before August 17, 2017, two counts of distributing indecent photos of a child and one offence of possessing an extreme pornographic image. Charles Myatt, prosecuting, said those offences were discovered after police had taken devices belonging to Hockley in relation to another offence - sexual communication with a child under 16 between April 2 2017 and May 8 2017 - which he was also convicted of. Hockley had been communicating with the girl, then aged under 12, on Facebook in a sexual way "totally inappropriate for a girl of that age".

Head teacher who groomed dozens of children on social media jailed

23/09/2022 - A British head teacher who groomed at least 131 children worldwide using social media has been jailed, the National Crime Agency (NCA) has said. Nicholas Clayton, 38 and from Wirral, used Facebook Messenger to contact children as young as 10, the NCA said. Children's charity the NSPCC voiced concerns that Meta, which owns Facebook, plans to introduce end-to-end encryption on its messaging platform. Andy Burrows, head of child safety online policy at the charity, said: "Clayton's case highlights the ease with which offenders can contact large numbers of children on social media with the intention of grooming and sexually abusing them." Private messaging is the frontline of child sexual abuse online. It's therefore concerning that Meta plans to press on with end-to-end encryption on Facebook Messenger, which will blindfold themselves and law enforcement from identifying criminals like Clayton.”

American gets 30 years in PH child porn case

16/07/2023 – WASHINGTON: A Chicago man has been sentenced to 30 years in prison for soliciting sexually explicit photos and videos from young girls in the Philippines. Karl Quilter, 58, pleaded guilty last year to sexual exploitation of children, the US Attorney’s Office for the North District of Illinois said.

Quilter enticed at least nine girls in the Philippines to produce sexually explicit photos and videos and send them to him via Facebook, Viber and Skype between 2017 and 2020, it said.

Man, 19, accused of offering and selling sex videos, nabbed in Cebu City

01/08/2022 - CEBU CITY, Philippines: A 19-year-old man, who was arrested for allegedly promoting and selling of self-produced videos of himself performing sexual acts to various male victims, including minors, underwent an inquest proceeding today, August 1, 2022. The National Bureau of Investigation Central Visayas Regional Office (NBI CEVRO) in a statement identified the accused as Romilo Romero, 19, a resident of Barangay Bulacao in Cebu City. On July 29, 2022, a composite team of the National Bureau of Investigation Anti-Human Trafficking Division (NBI AHTRAD), NBI CEVRO, Department of Justice Inter-agency Council Against Trafficking (DOJ IACAT) from Manila, DOJ IACAT-7, and the Department of Social Welfare and Development (DSWD) conducted these two pronged operations: an entrapment and rescue operation and to serve a warrant to search, seize, and examine computer data. Allegedly, Romero used social media platforms such as Facebook and Twitter to promote and sell sex videos.

PNP seeks court aid to track down sexual predators on social media

29/07/2022 - MANILA, Philippines: The Philippine National Police (PNP) has sought a regional trial court's permission to acquire information from social media giants Facebook and YouTube about the people behind "Usapang Diskarte" – an online account encouraging child sexual abuse.

UPDATE: Mother who pimped out 9 year old daughter jailed alongside 2 pedophiles

14/07/2022 - A mother was arrested yesterday for forcing her 9 year old daughter into prostitution. The 26 year old woman, Chantra, was arrested after she posted sexy pictures of herself on Facebook, adding she had a child sex video and underage sex photos for sale. The post soon went viral on social media resulting in members of the public contacting police. Chantra confessed a man contacted her via Facebook in April last year asking to have sex with her daughter in exchange for 3,000 baht. The woman says she took the money because her family was poor. The young mother drove to a hotel in Nakhon Pathom province to meet the man and recorded him having sex with her daughter. She confessed she sold it to other men via Facebook for 500 to 800 baht at a time.

Thai tutor arrested for making child porn with boys

18/07/2022 - An alleged pedophile wanted by the US and Thai Cyber police has finally been tracked down and arrested thanks to a local boxing gym owner. If found guilty the 20 year old part time teacher faces between three and 10 years imprisonment and a fine between 60,000 baht and 100,000 baht. The tutor, named Mai, sexually assaulted children between the ages of 7 and 15 years old, tricking them into making child pornography videos and making money by allegedly uploading them to the OnlyFans platform. A 31 year old woman named Somjit notified police that Mai promoted an OnlyFans account on Facebook, adding she was afraid he might sell child sex videos via that platform.

Convicted Sex Offender Sentenced to 20 Years in Prison for Child Pornography Offenses

12/07/2022 – BOSTON: A Greenfield man was sentenced today in federal court in Springfield for receiving child pornography. The defendant used Facebook messenger to communicate with a minor in the Philippines and receive pornographic images of the child. Fox induced a minor in the Philippines to engage in sexually explicit conduct for the purpose of producing images of that conduct. Specifically, Fox used Facebook messenger to communicate with the minor and to receive the pornographic images. In exchange for the images, Fox sent Western Union payments to the Philippines.

Former Montgomery County Teacher Pleads Guilty to Multiple Child Exploitation Offenses After Traveling to the Philippines to Have Sex with Children

29/06/2022 – PHILADELPHIA: United States Attorney Jacqueline C. Romero announced that Craig Alex Levin, 66, of King of Prussia, PA, pleaded guilty to six counts of child exploitation offenses before United States District Court Judge Harvey Bartle, III, stemming from his travel to the Philippines over a nearly three-year period for the purpose of engaging in illicit sexual conduct with minor children, some as young as 12 years of age. He also engaged in commercial sex trafficking by brokering the sale of a minor girl, who was pregnant at the time, for sex with an adult sex offender in exchange for money. Prior to and during his travels, Levin created and maintained Facebook accounts that he used to communicate with minors in the Philippines for the purpose of enticing them to engage in illicit sexual conduct with him during his visits to the island nation. In addition, the defendant used Facebook Messenger to send child pornography to minors in the Philippines.

St. Paul man sentenced to 43 years for largest sextortion case in FBI history

14/09/2022 - ST PAUL, Minnesota: According to the U.S. Department of Justice, from 2015 through 2020 Vang "adopted the personae of real minor girls" and posed as real people to get other young victims to produce and send him child pornography. When they refused, Vang threatened to and did release their sexually explicit images and videos. The FBI identified 1,100 minors targeted by Vang. There are victims in every state – including 50 in Minnesota – and in 13 other countries. The victims range from 12-17 years old. Born said Vang used dozens of usernames and IDs across different communications or social media platforms such as Skype, Snapchat, Facebook and Kik to lure minors into thinking that they were talking to another minor.

Exploiting Philippine minors through Facebook lands Texan in federal prison

25/05/2022 - BROWNSVILLE, Texas: A 47-year-old Harlingen man has been ordered to federal prison following his conviction of receiving child pornography, announced U.S. Attorney Jennifer B. Lowery. At the time of his plea, Machietto admitted that from Dec. 1, 2017, to June 1, 2018, he used Facebook to communicate with minor girls located in the Philippines. He requested nude photos of them and sent money as compensation to their families.

Former Federal Agent Found Guilty of Enticing a Minor and Engaging in Sex Tourism in the Philippines

23/05/2022 - East St. Louis, Illinois: A Cahokia, Illinois, man was found guilty as charged last week for Enticement of a Minor, Travel with Intent to Engage in Illicit Sexual Conduct, and Engaging in Illicit Sexual Conduct in a Foreign Place. According to evidence presented during trial, Joseph Albert Fuchs, III, an American citizen, met a 14-year-old girl while visiting the Philippines. Fuchs then engaged in sexual conversations with the minor using Facebook. During those conversations, Fuchs discussed ways to evade detection of her age when he would return to the Philippines to engage in sexual acts with her at a hotel. Fuchs then returned to the Philippines in March of 2019 and engaged in sexual acts with the 14- year-old minor.

Vallejo Man Pleads Guilty to Flying to the Philippines with the Intention of Engaging in Sexual Conduct with a Child

28/04/2022 - SACRAMENTO, California: Balbino Sablad, 80, of Vallejo, pleaded guilty today to traveling with the intent to engage in illicit sexual conduct, U.S. Attorney Phillip A. Talbert announced. According to court documents, in 2019, Sablad flew to the Philippines with the intention of engaging in sexual conduct with a child under the age of 16. Using Facebook, Sablad had engaged in sexual chats with a person he believed was the intended minor victim and he sent the intended minor victim over $2,000 prior to his travel to the Philippines. Before he arrived, he also discussed with a co-conspirator his plan to sexually abuse the intended minor victim in the Philippines.

Schemer using Facebook for sex with minors arrested in Iligan City

23/03/2022 - ILIGAN CITY, Philippines: A scheming netizen using Facebook to lure women into illicit sex was entrapped here Tuesday by agents of the National Bureau of Investigation. Dimaporo told reporters Austria would first offer women money in exchange for footages of them naked via online Messenger and threaten to circulate the obscene video clips if they refuse to have sex with him.

BBC Radio DJ Mark Page, 63, 'flew to the Philippines to have sex with girl, 13, sent graphic messages about what he wanted and asked a girl, 14, to carry out sex acts on a 12-year-old', court hears

02/03/2022 - A former radio executive allegedly flew to the Philippines to have sex with a 13-year-old girl and sent graphic messages about sex acts he wanted performed, a court has heard. Three of the offences were said to have occurred in 2016 on webcams, when he was in the UK and the children were in the Philippines, Teesside Crown Court was told. The remaining two offences were said to have happened in person after Page, who was also a DJ, travelled to the Philippines. Prosecutor Jo Kidd told the jury he set up a Facebook profile in the name of 'Thai G' and used it to contact a 13-year-old girl whilst in the Philippines in March 2019, before promising her 1,000 pesos. The court heard that Page sent graphic messages about sex acts he wanted the school children to perform.

Oil City Man Pleads Guilty to Child Sexual Exploitation Charge; Judge Detains Him Pending Sentencing

08/06/2021 - Brent Lockwood, 63, pleaded guilty to one count before United States District Judge Stephanie L. Haines. In connection with the guilty plea, the Court was advised that Lockwood received computer images depicting minors engaging in sexually explicit conduct. The Court was also advised that Lockwood repeatedly expressed, during Facebook chats, his desire to travel to the Philippines for the purpose of engaging in illicit sexual activity with minor females.

South Florida Man Sentenced to 25 Years in Federal Prison for Exploiting Poor Children in the Philippines

25/02/2022 - Miami, Florida: Dennis Pollard used a social media messenger application* in 2020 to find young girls in the Philippines whom he could groom for the purpose of producing child sexual abuse material (CSAM). Pollard offered, and sometimes provided, money through wire services in exchange for pornographic images of the girls. Over nearly six-weeks, Pollard convinced a 13-year-old girl, living in poverty, to record herself performing sexual acts in exchange for money. Pollard also directed a woman in the Philippines to record herself sexually abusing her two toddler-aged children. Pollard distributed CSAM of his victims to groom others and obtain more CSAM. In 2015, Pollard attempted to produce CSAM through a different account on the same social media messenger application.

Granite Falls man accused of possessing child pornography

17/02/2022 - Granite Falls, MN: James Leroy Sanborn, 85, of Granite Falls, MN is facing four felony charges for being a predatory offender allegedly possessing pornographic photos and videos involving minors. The images in his possession were allegedly sent to him by families in the Philippines that he was helping to support. According to the criminal complaint, Sanborn said during an interview that he might have images and videos on his phone and on his Facebook Messenger app. He said he sent money to five or six families in the Philippines. He said the money was to help them recover from fires and floods or send their children to school.

Teen girls duped into sending nude photos

05/02/2022 - Two men have been arrested in two locations for allegedly duping girls aged 13-15 to send them nude photos and videos of themselves in exchange for online game items. The arrests were made following complaints that some Facebook users had approached girls aged 13-15 to send their nude photos and videos in exchange for items that could be used in online games.