Question (Volume 2)	Your response
Please provide evidence to support your answer.	GeoComply's answer will be structured as follows: 1. Comments on pseudonymity and anonymity embolden offenders to engage in a number of harmful behaviours with a reduced fear of consequences. 2. Issues relating to the ability of perpetrators creating multiple fake user profiles to contact individuals against their will and circumvent blocking and moderation Online child sexual exploitation (OCSE) is an issue that is unfortunately enabled by the ability to operate and share data on the internet anonymously. Online offenders can easily circumvent the existing identity verification protocols on online platforms, facilitating and perpetuating online harm. **1. Comments on pseudonymity and anonymity emboldening offenders to engage in several harmful behaviours with a reduced fear of consequences.** GeoComply supports Ofcom in its assessment of the risks associated with pseudonymity and anonymity, which embolden offenders to engage in many harmful behaviours with a reduced fear of consequences. Online criminals tend to spoof or falsify identity and device data to operate anonymously online and evade oversight. Many social media companies report the volume of fake accounts they are actioning on their platforms. For example, in Q3 2023, Meta actioned 837 million fake accounts. Falsifying identifying information when establishing an account is mainstream and can be facilitated through anonymisation tools. An estimated 1.6 billion people use Virtual Private Networks (VPNs) globally, which encrypt internet traffic and redirect it through a specifically configured remote server run by a VPN host. Based on our experience operating in the geolocation and fraud detection space for over ten years, we know that cybercriminals may leverage various forms of location-altering technologies to hide their location and, therefore, their identity, allowing them to conduct illicit activities anonymously. Location obfuscation tools include (but are not limited to) Remote Desktops, Proxy

Question (Volume 2)	Your response
	Servers, TOR (The Onion Router) exit nodes, emulators, and jailbroken or rooted devices. Darknets, encryption services, and peer-to-peer (P2P) file-sharing services have created a safe harbour for offenders. The Virtual Global Taskforce affirms this: *'More offenders are using anonymizing technologies such as TOR as well as VPNs to commit sexual offences against children online.'* Without concrete, quality data relating to a user's profile, device, related accounts, or (as needed) identity information, social media platforms face tremendous obstacles in disrupting bad actors from conducting their illicit activity on their platforms. Moreover, law enforcement and regulators face barriers to investigating online criminal activity, which the WeProtect Global Alliance affirms: *'Even offenders with minimal technical knowhow can complicate the detection of crimes by using anonymisation solutions such as Tor and Virtual Private Networks (VPNs), which are now mainstream and built into some browsers by default. The overall effect is a significant hindrance to investigations caused by technologies with a low barrier to use.'* As highlighted by Ofcom in the chapter summary, such anonymisation tools are used for legitimate purposes, such as evading censorship or security. However, anonymisation tools are also readily available to bad actors who wish to circumvent identity protocols and establish fake accounts to conduct illicit activity online anonymously, such as sharing CSAM or other illicit content. **2. Issues relating to the ability of perpetrators creating multiple fake user profiles to contact individuals against their will and circumvent blocking and moderation** GeoComply applauds Ofcom for highlighting the issues relating to the ability of perpetrators to create multiple fake user profiles to contact individuals against their will and circumvent blocking and moderation. Despite reporting offending accounts, victims have been known to be re-victimised due to offenders' accounts either remaining active or the offender gaining

Question (Volume 2)	Your response
	access to the victim through separate accounts when the platform operators blocked, deleted, or removed the initial account. This issue, called device recidivism, leads to offenders being able to re-victimize children online and find new victims on platforms even when they have already been banned or removed by the platform. Offenders' ability to circumvent identity protocols on online platforms and set up fake accounts poses a threat to the safety and well-being of children. On the topic of the financial sextortion of children, C3P found that: *'Extorters can seemingly create multiple accounts that appear legitimate through careful curation or by hacking/taking over an existing account and repurposing it for their use. We believe extorters may also purchase stolen or hacked accounts from online communities dedicated to cybercrime. Victims have remarked that extorters often recycle the likeness of a profile, using the same images and name construction to operate multiple accounts simultaneously.'* Subsequently, strengthening identity verification protocols and the mechanisms used to prevent account recidivism is critically essential to disrupt and deter the use of electronic services to solicit, generate, distribute or access CSAM.
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.	*[Is this answer confidential? Yes / No (delete as appropriate)]*

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.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 8.2: Do you agree with the types of services that we propose the governance and accountability measures should apply to?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 9.1: 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 3)	Your response
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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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]	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

[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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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)]*
Question 11.3: Do you agree with our definition of large services?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 11.4: Do you agree with our definition of multi-risk services?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[2]	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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?	*[Is this answer confidential? Yes / No (delete as appropriate)]*

[2] See Annexes 7 and 8.

Question (Volume 4)	Your response
Question 12.1: 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 13.1: 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 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.	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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’?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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; • The ability of services in scope of the CSAM hash	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
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.	
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 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 (Volume 4)	Your response
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? • 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	*Is this answer confidential? No* GeoComply supports Ofcom’s efforts to block the accounts of users who share CSAM. To combat issues relating to blocking and preventing bad actors from returning to a service, GeoComply recommends leveraging device fingerprinting and authenticated multi-source geolocation data (GPS, Wi-Fi Triangulation, cellular, etc.) as part of authentication processes. In response to question 21.2, we address the advantages and disadvantages of leveraging device fingerprinting and geolocation to block and prevent a user from returning to a service. We offer comments based on our experience in geolocation, device and identity business-to-business software solutions. **1.1.Device fingerprinting** Device fingerprinting, or Fingerprinting-as-a-Service (FaaS), is a technique used to identify and flag devices on the internet. FaaS is commonly used as a means to fight fraud and authenticate identity. To create a unique device ‘fingerprint, ' information about a device's hardware and software configuration, such as operating system, browser, IP address, screen resolution, etc., is collected. Hardware and software indicators that might make up a device fingerprint vary between service providers, of which there are many in the market. Leveraging FaaS would enable platforms to flag devices associated with known suspicious and/or blocked users. This would prevent bad actors from being able to set up new accounts from the same device, regardless

Question (Volume 4)	Your response
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?	of the false aliases or identifiable information they use in the onboarding process to create or log into their accounts. Consequently, victims would be less at risk of being re-victimised by bad actors once they have been reported to the platform. In addition, FaaS would enable platforms to detect account hacking or takeovers, which is a tactic being deployed by offenders, in particular, to commit financial sextortion. For example, new login attempts with unknown/new devices might indicate fraud. Similarly, multiple accounts set up from one device could also be a risk indicator. In both cases, the activity could be flagged and escalated for additional authentication (for example, with two-factor authentication). One disadvantage of using FaaS to flag multiple accounts being set up from one device or a new device logging into an account is the risk of false positives. For example, in either scenario, a user could use a peer's device to log into their account. Fraud tools are only as good as the risk management frameworks in which they are deployed. Platforms can balance security with user access by establishing the correct and appropriate thresholds for suspicious user activity. Thresholds should be set and adapted through continuous and ongoing evidence and research. In addition, by combining several fraud detection tools and techniques in a broader risk management framework, platforms are in a more advantageous position to mitigate the disadvantages of each anti-fraud technique. For example, GeoComply's technology combines device integrity with multi-sourced geolocation analysis, among other fraud detection techniques, to identify, flag and prevent fraudulent activity in real time. **1.2.Geolocation** Multi-sourced geolocation data points, such as GPS, Wi-Fi Triangulation and GSM, enhance authentication processes by strengthening a platform's ability to identify anomalous user behaviour. Such data provides far more accurate and reliable location data sources than an IP address. Shortcomings associated with using IP for location include (but are not limited to): • The mainstream use of VPNs and proxies on the internet, which alter an IP address;

Question (Volume 4)	Your response
	- The growing use of relay proxies (such as Apple Relay or Google One), which are built into devices that billions of people use daily; - Dynamic IP addresses (i.e. those associated with mobile devices) do not indicate device location, often resolving back to carrier location; - Based on GeoComply data, the approximate range of an IP address is 100km. Consequently, we strongly recommend **against** relying upon an IP address to block/prevent users from reentering a service. Instead, by leveraging multiple geolocation data sources, such as GPS, Wi-Fi Triangulation, and GSM, a platform can cross-reference data points and ensure higher accuracy in locating an individual or device. Markets that embrace multi-source geolocation data in their Know Your Customer (KYC) processes (such as regulated online gaming in the U.S.) have demonstrated that online safety can be achieved while preserving privacy by leveraging third parties to authenticate identity who do not receive other personally identifiable information. In addition, coupling geolocation with FaaS helps mitigate the disadvantages of using only one technique. For example, the previously discussed scenario whereby a user logs into an account on their peer's device would be identified by leveraging geolocation. The platform would be able to identify that the user is logging on from a similar location to previous behaviour, thus determining that the transaction is not high risk. Alternatively, if a login attempt was made in a very different location and with an unknown device, it would be a higher risk. Furthermore, by leveraging geolocation in authentication, platforms could identify and manage suspicious locations and hotspots for illegal activity. For example, the United States' Federal Bureau of Investigations, Homeland Security Investigations and the National Center for Missing and Exploited Children issued a national public safety alert regarding an explosion in sextortion, identifying that a large proportion of schemes are originating out of West African countries such as Nigeria and Ivory Coast. By leveraging reliable, authenticated geolocation data, platforms can defend against organised criminal groups operating out of spe-

Question (Volume 4)	Your response
	cific locations. For example, the platform would be better equipped to reliably identify a login attempt from a flagged location associated with sextortion schemes without the risk of location spoofing or inaccuracy issues in the data. The platform would then determine the correct course of action, which could be enhanced due diligence or blocking the activity in real time. Similar to FaaS, one disadvantage of only relying on geolocation to prevent users from reentering a service is that of false positives. To mitigate this risk, platforms such as multi-factor authentication can leverage enhanced authentication checks (e.g. multi-factor authentication) for high-risk users, activities, and/or locations, or fraud mitigation techniques (e.g. FaaS) to assess risk and the correct cause of action. Collecting actionable and dynamic data both strengthen platforms' ability to: • Prevent bad actors from re-entering online platforms; • Stop the proliferation of fake accounts; • Strengthen record-keeping capabilities; and • Enhance the ability to identify criminals. As a non-biased, privacy-preserving strategy to ensure internet safety and strengthen authentication processes, multi-source geolocation and device data are critical parts of child exploitation investigations and increasingly vital tools for fraud detection. These data points enhance a user's risk profile without compromising their natural identity. In summary, steps available to mitigate the risk of victimisation from anonymous accounts include: • Identifying suspicious location patterns relating to online criminal behaviour by leveraging multi-sourced geolocation data for anti-fraud purposes; • Leveraging multi-sourced geolocation insights and device fingerprint technology to prevent offenders from victimising victims or repeatedly circumventing device and account-level bans; • Empowering platforms with greater actionable insights by integrating multi-source geolocation and anomalous behaviour detection into their existing risk management frameworks to

Question (Volume 4)	Your response
	protect children and better enforce platform terms of service; - Keeping records regarding risk management framework for harm reduction, enforcing terms of service, and preventing device recidivism.
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 for whom we propose to recommend more measures?	*[Is this answer confidential? Yes / No (delete as appropriate)]*
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	*[Is this answer confidential? Yes / No (delete as appropriate)]*

Question (Volume 4)	Your response
must have regard? If not, why not?	

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 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 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.