Your response

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response: We agree that having a named person responsible for managing risks and reporting to their board about illegal harms is a good idea, as it gives focus and accountability. Holding individuals to account is also easier than having a collective responsibility for an organisation, which can make enforcement harder.	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response: Board reporting should include analysis of the amount of fraud that occurs on the platform, to enable the organisation to carry out fraud mitigation measures. Platforms having a better understanding of fraud that originates on their platforms will help them to understand the role that they play. UK banks have published a number of reports on fraud origination online; the platforms should be able to source their own data to report on what they are seeing to provide their perspective.	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No	

Volume 4: What should services do to mitigate the risk of online harms

Automated content moderation (User to User)

Question 25:
i) Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response: We do not believe that costs to platforms to find and remove illegal content relating to fraud should be a barrier to most firms.
ii) Please provide the underlying arguments and evidence that support your views.
Response: With the costs of compute power lowering over time, and new tools such as AI to find even complex content, platforms should be able to build in robust content checking processes.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Default settings and user support for child users (U2U)

Question 31:
i) Do you agree with our proposals?
Response: Measure 7A: Default settings and support for child users (aka Age Verification). We broadly agree with the proposed approach, but think that measures for Age Verification (7A) should cover a broader range of platforms to maximise the protection of children online. Measure 7A only applies to large and small U2U platforms with specific risks of child grooming, and large platforms for search. This leaves the majority of platforms outside of the scope for this measure. A broader range of platforms should be in scope for age verification, to align the OSA with the ICO's Children's Code. All platforms in scope of a broadened OSA (even those not aimed at children) should assume that all unverified users are children, and provide child-safe content by default, unless the platform has obtained positive verification of age above a certain age, when the user can then be served content that is assessed for an older age group. This could be in

line with the PEGI age rating system, and would enable platforms to prove that they are complying with both the OSA and the ICO’s Children’s Code to simplify their compliance.

To gain access to adult content, including ‘harmful but legal’ content, users should be required to positively prove that they are over 18.

ii) Please provide the underlying arguments and evidence that support your views.

Response:

Making the internet ‘child safe’ by default, with users verifying as adults to get adult services, will greatly lower the risk that children are exposed to the kinds of harmful content that they see today.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Enhanced user control (U2U)

Question 37:

i) Do you agree with our proposals?

Response:

Measure 9C: Enhanced User Control (aka Identity Verification).

We broadly agree with the proposed approach, but think that measures for Identity Verification (9C) should cover a broader range of platforms to maximise the protection of individuals online.

Measure 9C only applies to large U2U platforms with multiple risks.

We agree with use of identity verification to give users more control over who they interact with, e.g. giving users the choice of only dealing with verified persons, but suggest the scope of platforms that should offer this should be broader to maximise safe online services. User verification should also be offered more broadly beyond just notable and paid accounts.

Platforms do not need to be mandated to verify users, but should be mandated to provide users with the *option* of being verified, to all users for free. We believe that this will make platforms safer and actually more attractive to users, who frequently are concerned about using social media due to the increase in scams. Having a safe platform is good for businesses and their brands.

There should be a mandated verification option that is free for the user (paid by the platform). If the platform can offer verification via a paid ‘premium’ account, that has low take-up, they could claim compliance with the OSA, but this will have ineffective outcomes. Some platforms offering verification as a paid feature today also charge the user costs that are far higher than the cost of verification, and are therefore not proportionate. Having a free verification feature option will maximise the benefits of this measure, and we expect that the majority of users would use it make themselves safe. Costs to the platform would be low compared to the benefits obtained, and therefore proportionate.

Features that should also be enabled once the user is verified:
Users should be able to clearly see who is verified, and who is unverified, on the platform. They should be able to filter out unverified users from both content feeds and contact suggestions, and to only present themselves to verified users (so they would be undiscoverable to unverified or fraudsters if they want to be).

Features that should be unavailable to unverified users:
Unverified users should not be allowed to trade or offer goods or services for sale; fraudsters take advantage of anonymous accounts to impersonate others, use synthetic ID names and disappear without delivering goods paid for. Requiring a verified account to trade should be standard practice, e.g. in the card scheme model, a merchant 'acquirer' provides a merchant account and is responsible for fraud carried out by its merchants. A similar approach could be used for platforms that want to capture value from trading; they should be liable for behaviour of their users. Verification brings with it accountability.

Platforms do not need to be 'real name visible'; pseudonymous accounts, with a verified person behind the pseudonym, enable increased privacy where desired. The verified personal data also does not all have to be shared with the platform; it could reside with a third party, with an identifier used to trace the actual user in case of enforcement. This increases privacy, data protection from hacks, and enables closer alignment with GDPR data minimisation principles. Too many platforms are starting to ask for full passport scans as part of verification, which will cause future problems when that data is exposed in breaches.

Ofcom should define what 'identity verification' means to ensure that platforms are carrying it out to a sufficient level of rigour. E.g. Twitter collecting a card payment does nothing to verify the user or stop bot accounts.

Platforms that enable trading should be required to educate and inform their users to only message each other via the platform, and not to move onto unsafe channels where contact details can be spoofed (e.g. phone, email, SMS). Payments should also be made via payment methods that have been enabled by the platform, that are safe and provide customer protection (which could be underwritten by the platform). Clear communications for users that they have protection for trades on-platform, and no protection if they move off of it, will reduce fraud. Ebay took this approach, successfully, when they owned PayPal.

ii) Please provide the underlying arguments and evidence that support your views.

Response: Impersonation fraud, purchase scams and many other fraud types are enabled by unverified accounts and spoofing of insecure channels. Verifying accounts brings accountability to them, and enables enforcement if account owners carry out illegal activity. It also prevents fraudsters from just opening new accounts whenever their unverified accounts are closed down; there is a higher cost for them to create new verified accounts, and it is much harder to do.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 38:

i) Do you think the first two proposed measures should include requirements for how these controls are made known to users?

Response: Yes, users should have full visibility of how to get verified, and of who else on the platform is verified. Transparency will maximise the effectiveness of the controls. If users cannot see who else is verified, they will continue to fall for scams from unverified/impersonation accounts.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 39:

i) Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?

Response: The value of verified accounts comes particularly for high-profile persons, such as footballers, who often get abuse from anonymous accounts. If the unverified anonymous accounts could be blocked from a feed or from posting/interacting with content, the person would not see the abuse. Increasing mental health issues from negativity on social media is a growing problem, leading to people disengaging completely as there is no 'safe' option without verification.

ii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Cumulative Assessment

Question 45:

i) Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?

Response:

We agree and support the OSA; broader use of age verification and identity verification will lead to better online safety for all users, and particularly children. For small companies providing U2U services online, being safe should not be prohibitive to their business models.

ii) Please provide the underlying arguments and evidence that support your views.

Response: N/A

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)

Response: No

Question 46:

i) 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?
Response: Yes, we consider the measures to be proportionate. Platforms with significant risks of illegal content should implement the measures to mitigate the risks.
ii) Please provide the underlying arguments and evidence that support your views.
Response: N/A
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Question 47:
i) We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response: Yes, large platforms have the resources to implement safer services and should lead by example.
ii) Please provide the underlying arguments and evidence that support your views.
Response: Profits for large platforms continue to grow via network effects. Making the large platforms safer will have a commensurate positive impact on their user bases.
iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No

Measure 7A: Default settings and support for child users (aka Age Verification)

Default settings are set to protect the child users:

- Children using a service are not presented with network expansion prompts, or included in network expansion prompts presented to other users.
- Children using a service should not be visible in the connection lists of other users. The connection lists of child users should also not be visible to other users
- Non-connected accounts do not have the ability to send direct messages to children using a service
- For services with no formal connection features, they should implement mechanisms to ensure children using a service do not receive unsolicited direct messages
- Location information of child users' accounts should not be visible to any other users via profile or content posts by default. In addition, any location sharing functionality should be 'opt in'

Applies to:

User to User services

Small platform, specific risks and Large platform, specific risks

d) Specific harm of grooming children for the purposes of sexual exploitation and abuse (CSEA). Measure does not apply to private communications or end-to-end encrypted communications. Measure recommended for services which:

i) are at high risk of grooming, or are large services at medium risk of grooming; and
ii) has an existing means of identifying child users.

The measure applies where the service has certain functionalities, as set out in the draft Codes.

Search services

Large platform, low risk

n) Measure recommended for general search services only, so excluding vertical search services
o) Measure recommended only when services have a predictive search functionality
p) We propose various measures for large general search services that technically apply if those services were low risk for all kinds of harm. However, we do not consider it realistic that such services would in practice be low risk for all kinds of harm without relevant measures.

Large platform, specific risks and Large platform, multiple risks

o) Measure recommended only when services have a predictive search functionality
p) We propose various measures for large general search services that technically apply if those services were low risk for all kinds of harm. However, we do not consider it realistic that such services would in practice be low risk for all kinds of harm without relevant measures.

Measure 9C: Enhanced User Control (aka Identity Verification)

There are clear internal policies for operating notable user verification and paid-for user verification schemes and improved public transparency for users about what verified status means in practice

Applies to:

User to User services

Large platform, multiple risks

h) Measure recommended for large services which:

i) are assessed as being at medium or high risk of either or both of fraud or the foreign interference offence; and
ii) label user profiles under one or more of the following: (i) a notable user scheme; or (ii) a monetised scheme.