Question	Your response
We welcome input from industry on the areas listed below. We encourage stakeholders to respond with feedback so that we can ensure that the guidance helps providers and other stakeholders understand:	
A) Ofcom's powers and providers' duties for transparency reporting, as well as Ofcom's approach to implementing the transparency regime. B) Ofcom's approach for determining what information service providers should produce in their transparency reports. C) Ofcom's plans to engage with providers prior to issuing transparency notices, and on what matters, and whether the proposed engagement plan will be sufficient for helping services to comply with their duties. D) Ofcom's plans to use the information in providers' transparency reports in Ofcom's own transparency reports.	We agree that transparency reports should include information on relevant risk factors, including risk factors identified under the illegal content and child safety risk assessment processes. Platforms should be required to report in detail on the presence and prevalence of risk factors which are relevant to their service, including breakdowns of number and nature of instances of harm associated with each risk factor, and actions taken in response. In the case of platforms' features, and functionalities which present risks, reports should also include information on the number and proportion of UK users making use of that feature or functionality and/or the number and proportion of UK users exposed to risks associated with it, the nature of that use and/or exposure to risk, and the number and nature of particular instances of actual harm. The cluster of features and functionalities which enable the creation of fake and/or anonymous user profiles has correctly been identified by Ofcom as a "stand out" risk factor in its draft illegal content risk register, and its draft children's risk profiles. Numerous pieces of research (including by Ofcom) have also found that there is also a good level of awareness amongst the general public of the risks associated with fake and

	anonymous accounts. Therefore, requiring platforms to offer greater transparency about the nature and scale of harms associated with fake and/or anonymous accounts has significant potential to drive improvements in safety. It can drive safety improvements directly through enabling greater scrutiny of platform's approaches, and through providing information and insights for Ofcom, and for independent civil society groups, which will help refine future regulatory guidance. For transparency around fake and anonymous accounts to fulfil this potential to drive safety improvements, the information required must be sufficiently specific and detailed. This is an area where platforms have a track record of evasion and obfuscation. For example in 2021 Twitter made claims about the link between anonymous accounts and racist abuse on its platform - to the press, to MPs, and to the Home Affairs Select Committee - that 99% of accounts which directed racist abuse at England Men's Team footballers during the Euros championship were "not anonymous". Twitter failed to respond to our requests for information to back up this claim, and it later emerged that Twitter had used an extremely misleading definition, which would consider as "not anonymous" an account with the username "Mickey Mouse", a made-up date of birth, the email address mickeymouseisnotreallymyname@gmail.com, and/or a number from a pay-as-you-go sim card bought from a newsagent for 99p.

	We suggest that Ofcom requires information relating to the presence of fake and anonymous accounts, and the prevalence of harms associated with these accounts, from any platform where this is a relevant risk factor. The information which Ofcom should require should include: • A breakdown of information collected by the platform during account/profile creation (e.g phone numbers, email addresses, linked accounts, name, address, date of birth, profile picture) • A breakdown of how any information collected is checked or verified • Where users are offered choices in what information to provide (e.g. whether or not to provide a phone number, or an address) and/or choices as to whether or not to verify or authenticate the information, a breakdown of the proportions of users who provided different information, the proportion for whom verification processes have been applied, and a breakdown of what those verification processes were • Where the platform conducts processes which it considers to be verification or authentication of a user's information or identity, evidence as to the effectiveness of the process (e.g records of information having been subsequently being found to be false) and any assessments or estimates of overall efficacy, and the platform's methodology for reaching these assessments • Any internal assessments or estimates of the proportion of profiles which map to real-world identities, those which are deliberately anonymous, and those

	which are inauthentic or intentionally deceptive; and their methodologies for reaching these assessments • Where platforms have in place policies in their terms and conditions relating to the authenticity of user profile information (e.g. Facebook's "real name" policy, or the rules against deception or impersonation present on many platforms) they should be required to set out what steps they take to ensure compliance with these policies; a detailed breakdown of the number and nature of actions to enforce compliance; an assessment of levels of non-compliance with these policies, by UK users and by accounts to which UK users are exposed; and their methodology for reaching these assessments • Any platform estimates or assessments of the numbers and proportions of users to whom a sanction has been applied (e.g. a suspension/ban/block) yet who are able to continue to use the platform using a different account, and their methodologies for reaching these assessments • Any platform assessments or estimates of the numbers of accounts purporting to be from the UK which are likely to be operated from outside the UK, and their methodology for reaching these assessments • Details of known instances of coordinated inauthentic behaviour involving, or targeting UK users, the numbers of users affected and the platform actions taken in response. Any platform assessments or estimates of levels of coordinated inauthentic behaviour and its reach to UK users, and

	their methodology for reaching these assessments • A detailed breakdown of harms where anonymous or fake accounts are a factor, the number of accounts involved, and the actions taken by the platform in response Confidential? – N

Please complete this form in full and return to OS-Transparency@Ofcom.org.uk