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.	Confidential? – N Under §77(3) of the Act, Ofcom has the ability to determine both the content that must be included in a transparency report, and the format in which it is presented - this presents a significant opportunity for enabling meaningful transparency. To maximise the effectiveness of the transparency regime, Ofcom should go beyond simply requiring service providers to provide high-level statistics about their systems, and should also require that data underpinning those statistics is made accessible to Ofcom, as well as the wider research community. Providing such access can be challenging due to privacy, security, and intellectual property concerns. However, there exists new infrastructure which can facilitate such data access whilst ensuring effective privacy and governance through the application of privacy enhancing technologies. The effectiveness of this infrastructure has been demonstrated by the Christchurch Call Initiative on Algorithmic Outcomes, which is discussed in further detail in our subsequent responses. We strongly encourage Ofcom to ensure relevant data is made accessible through the transparency reporting mechanism, and to explore the use of privacy-preserving infrastructure to facilitate this access.
Are there any aspects in the draft guidance where it would be helpful for additional detail or clarity to be provided?	Confidential? – Y/N
Are the suggested engagement activities set out in the draft guidance sufficient for providers to understand their duties and Ofcom's expectations?	Confidential? – Y/N

Question	Your response
We are also seeking input that will help us understand if there are other matters that Ofcom should consider in our approach to determining the notices, beyond those that we set out in the guidance. The questions below seek input about any additional factors Ofcom should take into account in various stages of the process, including: to inform the content of transparency notices; in determining the format of providers' transparency reports; and how the capacity of a provider can be best determined and evidenced.	
Are there any other factors that Ofcom might consider in our approach to determining the contents of notices that are not set out in the draft guidance?	Confidential? – Y/N
Is there anything that Ofcom should have regard to (other than the factors discussed in the draft guidance) that may be relevant to the production of provider transparency reports? This might include factors that we should consider when deciding how much time to give providers to publish their transparency reports.	Confidential? – Y/N
What are the anticipated dependencies for producing transparency reports including in relation to any internal administrative processes and governance which may affect the timelines for producing reports? What information would be most useful for Ofcom to consider when assessing a provider's "capacity", by which we mean, the financial resources of the provider, and the level of technical expertise which is available to the service provider given its size and financial resources?	Confidential? – Y/N
Are there any matters within Schedule 8, Parts 1 and 2 of Act that may pose risks relating to confidentiality or commercial sensitivity as regards service providers, services or service users if published?	Confidential? - N Whilst the actual disclosure risk will depend on the specific context, the fact that many of the matters outlined in Schedule 8 relate to providing information about either users (e.g. "The number of users who are assumed to have encountered illegal search content or search content that is harmful to children") or the system design (e.g. "The design and operation of algorithms which affect the display, promotion, restriction or recommendation of

	illegal content") means that there is a general risk that requests for such information are challenged due to concerns around data privacy, confidentiality, or commercial sensitivity. At the same time, making such information accessible is crucial for meaningful platform transparency. OpenMined has worked on developing freely available open-source infrastructure that seeks to overcome this tension between transparency and confidentiality, by facilitating structured access to proprietary data and AI systems. This infrastructure can enable access whilst protecting privacy, security, and IP by design through the use of privacy enhancing technologies. This tension between transparency and confidentiality also motivated the establishment of the Christchurch Call Initiative on Algorithmic Outcomes by the governments of France and New Zealand, which has utilised this infrastructure to enable sensitive platform data to be made accessible for independent research into TVEC and other online harms, whilst guaranteeing the privacy and security of the data. This has been piloted to facilitate research into the impacts of production recommender systems at Microsoft's LinkedIn and Dailymotion. We encourage Ofcom to explore leveraging similar infrastructure as a way to maximise the operationalisation of its transparency regime. Without this, it is likely that requests for information under Schedule 8 will face onerous legal challenges.

Question	Your response
Finally, we are also seeking input into any matter that may be helpful for ensuring Ofcom's transparency reports are useful and accessible.	
Beyond the requirements of the Act, are there any forms of insight that it would be useful for Ofcom to include in our own transparency	Confidential? – Y/N

reports? Why would that information be useful and how could you or a third party use it?	
Do you have any comment on the most useful format(s) of services' transparency reports or Ofcom's transparency reports? How can Ofcom ensure that its own transparency reports are accessible? Provide specific evidence, if possible, of which formats are particularly effective for which audiences.	Confidential? – N We support Ofcom's ambition to leverage individual transparency reports in its own transparency reporting in order to provide researchers and citizens with industry-wide insights, offer comparability between services, understand changes over time, and highlight best practices and gaps across the industry. §5.5 of the guidance states that Ofcom will convert data into insight - whilst we agree that it is important for Ofcom to do this, it is also vital that Ofcom is able to use its authority to extend access to the data itself to a broader set of researchers. This can enable the discovery of much richer insights into online harms and safety mechanisms. Ofcom could establish similar infrastructure to that outlined in our response to the previous question in order to facilitate access, particularly for data which may be sensitive. Leveraging transparency reporting to make such data accessible could also be a powerful recommendation of the report on researchers' access to information that Ofcom is required to produce under S. 162 of the Act. Significant insights can be gleaned from this transparency data, but we also wish to highlight that there exists a class of research questions that can only be answered if such data is linkable across platforms, for example if we want to fully understand how a particular disinformation narrative spreads across different platforms. Furthermore, there are research questions that can only be answered if platform data can be linked with third-party data - for example, if we want to understand the impacts of algorithms across different demographic groups then we would need to link platform data with demographic data from e.g. the ONS. Often, such linkage is not possible as it requires the disclosure of identifiers which constitute personal data (e.g. a user ID or username), and sharing such information is blocked due to (real or perceived) risks of

	breaching UK data protection law. Fortunately, there now exists mature technologies (e.g. secure enclaves*) which can facilitate privacy-preserving record linkage. Such technologies are readily integrated into the infrastructure we described previously, and we implore Ofcom to explore these features as part of their transparency regime. ** A secure enclave is a new type of computer chip manufactured with a cryptographic private key inside; no one can get to that key without breaking the chip, such that no one can obtain the private key. The secrecy of this key means that external parties can encrypt data in a way that only this chip can decrypt. When an enclave is attached to the internet, multiple parties can send data from around the world to the enclave and be confident that their data can only be decrypted inside the enclave. Thus, records can be linked inside the enclave without disclosing sensitive information to other parties.*

Question	**Your response**
Please provide any other comments you may have.	
General comments	Confidential? – Y/N

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