10 March 2025

Ofcom
Riverside House
2a Southwark Bridge Road
London
SE1 9HA

Via Email: technologynotices@ofcom.org.uk

Re: Technology Notices Consultation

Dear Ofcom,

Thank you for the opportunity to respond to this consultation. Before providing our substantive responses to the questions posed, we wish to set out some context that we would like Ofcom to consider in its development of this proposal.

Our policies and enforcement principles are grounded in human rights. X has robust policies in place to address terrorist and child sexual exploitation and abuse (CSEA) content, including under our child sexual exploitation and violent and hateful entities policies. Our content moderation systems are designed and tailored to mitigate systematic risks without unnecessarily restricting the use of our service and fundamental rights, especially freedom of expression. We enforce through content moderation activities, which are implemented and anchored on principled policies and leverage a diverse set of interventions to ensure that our actions are reasonable, proportionate and effective.

Privacy is a fundamental right and for X, protecting privacy is a priority. We enforce strict measures to safeguard personal privacy and prevent unauthorised disclosures. With regard to the use of accrediting technology for end-to-end- encrypted (E2EE) services, we have significant concerns and request confirmation from Ofcom that E2EE services will not be subject to TNs. As is outlined by Amnesty International[1], encryption is a crucial enabler of human rights and essential means of protecting private information. Any proactive scanning that involves

---

[1] https://www.amnesty.org/en/documents/pol40/3682/2016/en/

identifying specific pieces of content compromises E2EE, undermining the privacy and security of individuals and as such, individual human rights.

Ofcom should be mindful of the significant concerns raised with regard to UK user privacy and international repercussions in response to the recent issuing of a Technical Capability Notice to Apple under the UK's Investigatory Powers Act 2016 demanding access to Apple users' encrypted data. We also note that creating back-door access to E2EE may have unintended consequences, for example, undermining security risks opening up private data to infiltration from bad actors and for malicious purposes.

As we outline in further detail below, we urge Ofcom to consider the interaction between the use of TNs and any potential conflict with other legislative frameworks. For example, the interaction with UK GDPR requirements, as well as the interaction with global regulatory regimes in situations where UK users are communicating with users outside of the UK.

Freedom of expression is core to X's mission. We welcome that the protection of privacy and freedom of expression is specifically protected under Section 22 of the UK Online Safety Act: *"When deciding on, and implementing, safety measures and policies, a duty to have particular regard to the importance of protecting users' right to freedom of expression within the law."* With regard to audit-based assessments, we recommend any impact on freedom of expression is given detailed consideration during this stage to avoid a situation whereby inaccurate tech results in wrongful action on accounts/content, and subsequently interferes with free expression.

Furthermore, as noted in more detail below, while we are supportive of the inclusion of independent performance testing, we are concerned with a sole reliance on benchmarking. We recommend that benchmarking is complemented with a prescribed threshold for performance testing outcomes.

We note that Ofcom's draft guidance lacks clarity on "necessity' and 'proportionality' with regard to the practical use of measures and request clarity on such.

Finally, we request confirmation from Ofcom that providers will be involved in decision-making processes with regard to the use of TNs; confirmation that we will be able to nominate a skilled person; and that clarity on timeframes for taking action to comply with TNs are provided.

For the reasons stated above and as explained fully in the Annex below, we respectfully suggest that the proposal be reconsidered. We look forward to further engaging with Ofcom on this important issue.

Sincerely,

Twitter International Unlimited Company

Question	Your response
Question 1: Do you have any views on our audit-based assessment, including our proposed principles, objectives, and the scoring system? Please provide evidence to support your response	• The interaction with other legislative frameworks should be more thoroughly considered during the audit stage, allowing developers the opportunity to address any concerns upfront, rather than waiting until Ofcom is determining whether to issue a Technology Notice (**TN**). In the UK, TNs have the potential to conflict with the UK GDPR and interception/ confidentiality of communications regimes in particular, unless the technology and its deployment is carefully assessed. It is also very difficult to deploy a scanning technology without a knock-on impact on users in other jurisdictions as well (e.g. users communicating with UK users via private channels) which could risk putting X in breach of those global regimes, and this should be considered up-front. • As a public body under the Human Rights Act (**HRA**) 1998, Ofcom is legally obligated to act compatibly with the European Convention on Human Rights, including safeguarding freedom of expression and privacy and ensuring its regulatory decisions respect and uphold these fundamental rights in all proceedings and policies. Human rights need to be considered in more detail at the audit stage. By way of example, inaccurate tech can lead to more false positives, resulting in wrongful action on accounts/content, inaccurate reports to the National Crime Agency, and therefore interference with free expression. • The fact core accuracy metrics like precision/recall are only a factor in the audit-based assessment, without a firm minimum accuracy threshold being required, could result in technologies with low core accuracy metrics being passed. We suggest introducing a minimum precision/recall threshold at the audit stage to avoid this outcome. Our comment on the impact of inaccuracy on free expression noted above applies here also. Any minimum threshold should be set at a level that considers the impact on large services like X, where a drop in accuracy (e.g., from 80% to 70%) leads to a significant increase in inaccurate reports, with real-world consequences for users. We urge Ofcom to factor this into their decision when establishing thresholds.

	scanning technology without a knock-on impact on users in other jurisdictions as well (e.g. users communicating with UK users via private channels) which could risk putting X in breach of those global regimes, and this should be considered up-front.
	● As a public body under the Human Rights Act (**HRA**) 1998, Ofcom is legally obligated to act compatibly with the European Convention on Human Rights, including safeguarding freedom of expression and privacy and ensuring its regulatory decisions respect and uphold these fundamental rights in all proceedings and policies. Human rights need to be considered in more detail at the audit stage. By way of example, inaccurate tech can lead to more false positives, resulting in wrongful action on accounts/content, inaccurate reports to the National Crime Agency, and therefore interference with free expression.
	● The fact core accuracy metrics like precision/recall are only a factor in the audit-based assessment, without a firm minimum accuracy threshold being required, could result in technologies with low core accuracy metrics being passed. We suggest introducing a minimum precision/recall threshold at the audit stage to avoid this outcome. Our comment on the impact of inaccuracy on free expression noted above applies here also.
	● Any minimum threshold should be set at a level that considers the impact on large services like X, where a drop in accuracy (e.g., from 80% to 70%) leads to a significant increase in inaccurate reports, with real-world consequences for users. We urge Ofcom to factor this into their decision when establishing thresholds.
Question 2: Do you have any views on our proposals for independent performance testing, including the two mechanisms for setting thresholds; the approach to testing technologies in categories against particular metrics; and data considerations? Please	● We support the inclusion of independent performance testing given this is important to ensure the technology works in specific deployment contexts. Otherwise, we fear Ofcom would only be accrediting technologies based on metrics self-reported by developers at the audit stage. This being said, relying solely on

provide evidence to support your response.	benchmarking could lead to Ofcom accrediting the least problematic options or the "best of a bad bunch". In our view, a more effective approach would be to complement benchmarking with a prescribed threshold for performance testing outcomes. ● As noted above, any minimum threshold should be set at a level that takes into account the largest services like X. ● Accrediting technology for E2EE service types (and, by extension, requiring independent performance testing for these services) is not appropriate. Proactive scanning that involves identifying specific pieces of content cannot be achieved without compromising end-to-end encryption.
Question 3: Do you have any comments on what Ofcom might consider in terms of how long technologies should be accredited for and how often technologies should be given the opportunity to apply for accreditation? Is there any further evidence we should consider?	We suggest implementing certain safeguards such as: ● methods for continuous evaluation, including performance on X in particular (rather than hypothetical services during the audit/testing phase); ● clear guidelines on whether failing to achieve accreditation standards leads to the revocation of the TN; and ● ensuring the independence of designated third parties conducting the audits.
Question 4: Do you have any views on how to turn these proposals into an operational accreditation scheme, including the practicalities of submitting technology for accreditation? Is there any additional evidence that you think we should consider? Please provide any information that may be relevant.	
Question 5: Do you have any comments on our draft Technology Notice Guidance?	● This draft guidance lacks detail on how Ofcom will consider necessity and proportionality in practice, and we encourage Ofcom to give some more clarity/specific examples here – particularly around how you will weigh up the "Specified Matters". ● We refer again to your HRA duties (and the fact that insufficiently clear legislation may render any interference with user rights unlawful). In particular, we expect more clarity on how Ofcom will consider (i) effectiveness of providers' existing safety measures; and (i) technical

	feasibility of design/operational changes to a service.

- We seek clarity from Ofcom that E2EE services will not be subject to a TN, taking human rights considerations into account.

- See our point in response to Question 1 regarding the interaction (and potential conflict) with other UK and global digital regulatory regimes.

- We would also like to use this opportunity to seek:
  - assurances that you will involve providers in the decision-making process (this is not clear to us currently);
  - confirmation that we will be able to nominate a skilled person; and
  - longer periods to make representations/clarity on timeframes for taking action to comply with TNs, with emphasis on the inevitable operational/technical challenges for a large provider implementing a TN. |