Your response

Question	Your response
Question 1: How do you measure the number of users on your service?	Confidential? – Y / N
Question 2: If your service comprises a part on which user-generated content is present and a part on which such content is not present, are you able to distinguish between users of these different parts of the service? If so, how do you make that distinction (including over a given period of time)?	Confidential? – Y / N
Question 3: Do you measure different segments of users on your service? ● **Do you segment user measurement by different parts of your service? For example, by website vs app, by product, business unit.** ● **Do you segment user measurement into different types of users? For example: creators, accounts holders, active users.** ● **How much flexibility does your user measurement system have to define new or custom segments?**	Confidential? – Y / N
Question 4: Do you publish any information about the number of users on your service?	Confidential? – Y / N

Question	Your response
Question 5: Do you contribute any user number data to external sources/databases, or help industry measurements systems by tagging or sharing user measurement data? If not, what prevents you from doing so?	Confidential? – Y / N
Question 6: Do you have evidence of functionalities that may affect how easily, quickly and widely content is disseminated on U2U services? ● **Are there particular functionalities that enable content to be disseminated easily on U2U services?** ● **Are there particular functionalities that enable content to be disseminated quickly on U2U services?** ● **Are there particular functionalities that enable content to be disseminated widely on U2U services?** ● **Are there particular functionalities that prevent content from being easily, quickly and widely disseminated on U2U services?**	Confidential – N Within the "attention economy",[1] many commercial U2U services seek to maximise user engagement with paid content by encouraging users to spend more time on their platforms (see question 8 for further commentary). This business model incentivises U2U services to implement features and functionalities that boost both organic and paid content in order to maximise the attention of the user and therefore maximise ad revenue. These features and functionalities mean that content is disseminated more easily, quickly and widely. While, as an NGO rather than a U2U service, we do not have direct empirical evidence as to how each functionality impacts the dissemination of content on U2U services, we encourage Ofcom to consider the following types of functionalities in its categorisations: ● Functionalities which encourage users to disseminate content with other users and onto other platforms, including: ○ Prominent placement of share buttons, sometimes functioning as nudges or dark patterns[2] prompting users to like, share, repost, subscribe or take some other action, or rewarding them for doing so; ○ Features allowing users to share with users beyond their contacts or friends lists, such as "public" vs. "private" sharing settings;

[1] See Center for Human Technology. The Attention Economy Why do tech companies fight for our attention? Available at: https://assets.website-files.com/5f0e1294f002b15080e1f2ff/612f8e3fa20df8374659a774_1%20-%20The%20Attention%20Economy%20Issue%20Guide.pdf

[2] Dark patterns often take advantage of consumers' cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions. For more information, see see Federal Trade Commission. Bringing Dark Patterns to Light (2022). Available at: https://www.ftc.gov/reports/bringing-dark-patterns-light; European Data Protection Board. Guidelines on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 (2023). Available at: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

Question	Your response
	○ Allowing users to share or forward content to large groups, channels or lists of people, sometimes of unlimited sizes. ● Functionalities which seek to maximise the time spent by users on the service, which in turn increases the rate at which content is consumed and disseminated across the network and the total number of users it is viewed by; for example: ○ Using content ranking and content distribution algorithms that disseminate content towards users according to their interests, networks or usage patterns, based on data collected on each user; ○ Auto-playing videos without needing action from the users; ○ "Endless" feeds where the users can keep scrolling forever; ○ Rewarding users with "streaks" or points for consecutive days or hours where they have engaged with the service; ○ Pushing notifications to users' devices; ○ Featuring "stories" or other time-limited content which prompts continuous engagement to avoid missing out. ● Functionalities which encourage or facilitate "virality" of timely or trending content, maximising user engagement with a particular topic or event and rapidly disseminating content shared under that theme; ○ Using hashtags, alerts or labels which index relevant content; ○ Content ranking algorithms which reward content which many people are engaging with by promoting it amongst broader audiences; ○ Content promotion algorithms which allow platform employees to amplify or boost particular content to broader audiences (e.g. TikTok's "heating" button[3]) ● Functionalities which allow advertisers to maximise engagement with ads, disseminating paid content more widely and effectively; ○ Providing targeted advertising algorithms allowing advertisers to target users with particular addresses, gender, age,

[3] See Mitchell Clark. TikTok confirms that its own employees can decide what goes viral. The Verge (January 20, 2023). Available at: https://www.theverge.com/2023/1/20/23564242/tiktok-heating-view-boosts-creators-businesses

Question	Your response
	interests, education or a range of other characteristics; ○ A/B testing of ad messages by the service provider to determine how to trigger a higher click rate by users; ○ Promotional posts, for example by influencer accounts with lots of followers. Conversely, some functionalities can be used to prevent content from being disseminated easily, quickly and widely on U2U services. Such functionalities may be implemented either to address harmful content, to protect private or subscription-only content, or simply to improve the quality of user engagement and experiences rather than maximising clicks or views with as much content as possible.[4] These include: ● Functionalities which reduce or minimise the time spent by users on the U2U service, reducing the overall engagement with and dissemination of content on the service. For example: ○ Features which limit the time each user spends on the service, or the amount of content that a user can consume in a single time window[5]; ○ Reminders to "take a break" or warnings about the time the user is spending on the service; ○ Minimising notifications, and avoiding using bright colours or flashing icons which attract the user to the service[6]; ● Functionalities which introduce a layer of "friction"[7] making it harder for users to share or repost content. These might include: ○ Preventing users from sharing media without having read or watched it first;

[4] In some cases, implementation of these functionalities may be economically beneficial (for example, ensuring that illegal content is not displayed next to paid ads, or encouraging users to subscribe to have access to particular content). In other cases, implementation of these functionalities may require economic incentives to be deprioritised in the interests of user safety. (see question 8 for further commentary)

[5] See Zeyi Yang. How China takes extreme measures to keep teens off TikTok. MIT Review (March 8, 2023). Available at: https://www.technologyreview.com/2023/03/08/1069527/china-tiktok-douyin-teens-privacy/#:~:text=On%20March%201%2C%20TikTok%20announced,make%20that%20decision%20for%20themselves

[6] See David Nield. Try Grayscale Mode to Curb Your Phone Addiction. Wired (1 December, 2019) Available at: https://www.wired.com/story/grayscale-ios-android-smartphone-addiction/

[7] Jahn, Laura & Kræmmer Rendsvig, Rasmus & Flammini, Alessandro & Menczer, Filippo & Hendricks, Vincent. Friction Interventions to Curb the Spread of Misinformation on Social Media (2023). Available at: https://www.researchgate.net/publication/372547505_Friction_Interventions_to_Curb_the_Spread_of_Misinformation_on_Social_Media

Question	Your response
	○ Having users complete CAPTCHAS, quizzes or other tasks before sharing a piece of content; ○ Preventing users from sharing with users beyond their contacts or friends lists, and/or encouraging users to share only with close friends or lists of "favourites"; ○ Preventing users from forwarding to large groups, channels or lists of people, or limiting the number of times that a file can be shared by a single user. ● Functionalities limiting access to certain content for certain groups of people. For example: ○ Paywalls to block sharing with non-subscription-paying users; ○ Providing the service only for users in a particular locale, country or region rather than having a global scope; ○ Age-gating mechanisms that prevent underage users from viewing or interacting with particular content or users.[8] ● Functionalities which identify certain content types and limit their dissemination or visibility and/or remove the content entirely. This might include: ● Features which allow human moderators to flag or remove content which is impermissible under platform guidelines ● Features which allow automated systems to flag or remove content which is impermissible under platform guidelines ● Features which allow community members, trusted flaggers or users to flag, report or label suspicious or harmful content[9] ● Features which limit the dissemination of content which has been forwarded many times already.[10]

[8] Please note that such mechanisms do pose as yet unaddressed risks to privacy and freedom of expression, as detailed in our previous submission from March 2023. Available at: https://gp-digital.org/wp-content/uploads/2023/06/GPD-Ofcom-submission-March-2023.pdf

[9] a solution that has proven limited depending on how the flagging or labelling is conducted, what are the human resources put in place, what are the guidelines to execute it, how the external advisors are selected, among others. See Orestis Papakyriakopoulos and Ellen Goodman. The Impact of Twitter Labels on Misinformation Spread and User Engagement: Lessons from Trump's Election Tweets. In Proceedings of the ACM Web Conference (2022). Association for Computing Machinery, New York, NY, USA, 2541–2551. Available at: https://doi.org/10.1145/3485447.3512126

[10] Nathalie- Ann Hall et al. Beyond Quick Fixes How Users Make Sense of Misinformation Warnings on Personal Messaging (2023). Available at: https://www.lboro.ac.uk/research/online-civic-culture-centre/news-events/articles/o3c-4-beyond-quick-fixes/

Question	Your response
	[N.B. Caution should always be exercised in developing, testing and implementing functionalities designed to identify and limit/remove certain content types; particularly where such systems rely on algorithms with limited accuracy which may risk reducing content which should be permissible under international human rights law.[11] Please see our submission to Ofcom's call for evidence: first phase of online safety regulation (September 2022) for more information; in particular the responses to Qs 11, 14 and 22.[12] Footnotes 1. See Center for Human Technology. The Attention Economy Why do tech companies fight for our attention? Available at: https://assets.website-files.com/5f0e1294f002b15080e1f2ff/612f8e3fa20df8374659a774_1%20-%20The%20Attention%20Economy%20Issue%20Guide.pdf 2. Dark patterns often take advantage of consumers' cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions. For more information, see see Federal Trade Commission. Bringing Dark Patterns to Light (2022). Available at: https://www.ftc.gov/reports/bringing-dark-patterns-light; European Data Protection Board. Guidelines on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 (2023). Available at: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf 3. See Mitchell Clark. TikTok confirms that its own employees can decide what goes viral. The Verge (January 20, 2023). Available at: https://www.theverge.com/2023/1/20/23564242/tiktok-heating-view-boosts-creators-businesses 4. In some cases, implementation of these functionalities may be economically beneficial (for example, ensuring that illegal content is not displayed next to paid ads, or encouraging users to subscribe to have access to particular content). In other cases, implementation of these functionalities may require economic incentives to be deprioritised in the interests of user safety. (see question 8 for further commentary) 5. See Zeyi Yang. How China takes extreme measures to keep teens off TikTok. MIT Review (March 8, 2023). Available at: https://www.technologyreview.com/2023/03/08/1069527/china-tiktok-douyin-teens-privacy/#:~:text=On%20March%201%2C%20TikTok%20announced,make%20that%20decision%20for%20themselves 6. See David Nield. Try Grayscale Mode to Curb Your Phone Addiction. Wired (1 December, 2019) Available at:

[11] See Joint statement from more than 300 scientists from 32 countries warning against the EU proposal for regulation to detect Child Sexual Abuse Material (2023). Available at: https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit

[12] https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf

Question	Your response
	https://www.wired.com/story/grayscale-ios-android-smartphone-addiction/ 7. Jahn, Laura & Kræmmer Rendsvig, Rasmus & Flammini, Alessandro & Menczer, Filippo & Hendricks, Vincent. Friction Interventions to Curb the Spread of Misinformation on Social Media (2023). Available at: https://www.researchgate.net/publication/372547505_Friction_Interventions_to_Curb_the_Spread_of_Misinformation_on_Social_Media 8. Please note that such mechanisms do pose as yet unaddressed risks to privacy and freedom of expression, as detailed in our previous submission from March 2023. Available at: https://gp-digital.org/wp-content/uploads/2023/06/GPD-Ofcom-submission-March-2023.pdf 9. a solution that has proven limited depending on how the flagging or labelling is conducted, what are the human resources put in place, what are the guidelines to execute it, how the external advisors are selected, among others. See Orestis Papakyriakopoulos and Ellen Goodman. The Impact of Twitter Labels on Misinformation Spread and User Engagement: Lessons from Trump's Election Tweets. In Proceedings of the ACM Web Conference (2022). Association for Computing Machinery, New York, NY, USA, 2541–2551. Available at: https://doi.org/10.1145/3485447.3512126 10. Nathalie- Ann Hall et al. Beyond Quick Fixes How Users Make Sense of Misinformation Warnings on Personal Messaging (2023). Available at: https://www.lboro.ac.uk/research/online-civic-culture-centre/news-events/articles/o3c-4-beyond-quick-fixes/ 11. See Joint statement from more than 300 scientists from 32 countries warning against the EU proposal for regulation to detect Child Sexual Abuse Material (2023). Available at: https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit 12. https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf
Question 7: Do you have evidence relating to the relationship between user numbers, functionalities and how easily, quickly and widely content is disseminated on U2U services?	Confidential – N To our knowledge, most empirical research on the relationship between user numbers, platform functionalities and the spread of content is specific to individual content-types – such as abuse, disinformation or child sexual abuse material – or individual events or topics, such as elections or health concerns. It is therefore difficult to comment or gather evidence on how user numbers and functionalities impact the dissemination of *all* content types across *all* platforms in general.

Question	Your response
	For example, an Alan Turing Institute Report on online abuse from 2019[13] found that the prevalence of abuse was less than 1% on mainstream platforms, but between 5 and 8% in niche alternative spaces. Yet the size of the mainstream platforms might mean that the abusive content was more widely disseminated to a higher number of users, despite the lower prevalence, whereas conversely in niche alternative spaces the abusive content may have been disseminated less widely. It is important to collect data from platforms not only on the number of users that use the service, but also the number of users that see or engage with different types of content and the average amount of time a user spends on the service, to gain a more nuanced picture of how user numbers and functionalities impact the dissemination of content on that service. Early research on this topic did suggest that the dissemination of content may depend somewhat on "trust relationships between users", with users more likely to re-share or amplify content from peers or individuals who they like or admire.[14] In this sense, it may also be useful to examine the strength of network effects within and across different U2U services as a factor driving the rapid dissemination of content. Footnotes 13. Bertie Vidgen et. al. How much online abuse is there? A systematic review of evidence for the UK Policy Briefing (2019) Available at: https://www.turing.ac.uk/sites/default/files/2019-11/online_abuse_prevalence_full_24.11.2019_-_formatted_0.pdf 14. Arnaboldi, Valerio et al. The Role of Trusted Relationships on Content Spread in Distributed Online Social Networks (2014) Available at: https://www.researchgate.net/publication/277501318_The_Role_of_Trusted_Relationships_on_Content_Spread_in_Distributed_Online_Social_Networks
Question 8: Do you have evidence of other objective and measurable factors or characteristics that may be relevant to category 1 threshold conditions?	Confidential – N As mentioned in the answer to question 6, many of the functionalities that drive the rapid dissemination of content on U2U services are driven by a business model which is attached to maintaining user engagement and

[13] Bertie Vidgen et. al. How much online abuse is there? A systematic review of evidence for the UK Policy Briefing (2019) Available at: https://www.turing.ac.uk/sites/default/files/2019-11/online_abuse_prevalence_full_24.11.2019_-_formatted_0.pdf

[14] Arnaboldi, Valerio et al. The Role of Trusted Relationships on Content Spread in Distributed Online Social Networks (2014) Available at: https://www.researchgate.net/publication/277501318_The_Role_of_Trusted_Relationships_on_Content_Spread_in_Distributed_Online_Social_Networks

Question	Your response
	attention for as long as possible in order to generate more advertising revenue. The landscape is further complexified by the use of micro-targeting and automated advertising systems that are deployed by the U2U service to maximise the capture of users' attention and charge higher prices to advertisers for customised or personalised advertising.[15] Where a content ranking or recommendation algorithm is designed to maximise profit and user engagement rather than focusing on the health of the information environment, it will inevitably produce systems which amplify and promote the spread of divisive, shocking or disturbing content. Conversely, some U2U services even with very many users which are underpinned by different business models (such as publicly funded or not-for-profit services) tend to collect far less personal or behavioural data from users and not to use such data for the purposes of personalised content or ad targeting. In light of the absence of an exemption for public interest platforms in the Online Safety Bill,[16] we believe that as well as considering particular functionalities and numbers of users for the purpose of categorising U2U services into Cat 1 and Cat 2, the following factors may also be relevant: ● The amount of personal data collected by U2U services, for example the number of data points, characteristics or behaviours that are used to inform the U2U service's personalisation algorithms for organic and paid content; ● The proportion of service revenue that is generated by ad placements; ● The average amount of time that an average user spends on the service, and/or the percentage of content that the user views that they did not directly request or seek out. See, for example, Kevin Roose's research on the harmful properties

[15] Research ICT Africa, Digital Governance and the challenges for trust and safety. Part 1 (2023). Available at : https://researchictafrica.net/wp/wp-content/uploads/2023/02/Part-1-.pdf. Also see Carlos Carrasco-Farré, 'The Fingerprints of Misinformation: How Deceptive Content Differs from Reliable Sources in Terms of Cognitive Effort and Appeal to Emotions', Humanities and Social Sciences Communications 9, no. 1 (9 May 2022): 1–18, https://doi.org/10.1057/s41599-022-01174-9; Ullrich K. H. Ecker et al, 'The psychological drivers of misinformation belief and its resistance to correction', 2022, https://www.nature.com/articles/s44159-021-00006-y.pdf; Lan Ha, Timothy Graham, and Joanne Gray, 'Where Conspiracy Theories Flourish: A Study of YouTube Comments and Bill Gates Conspiracy Theories', Harvard Kennedy School Misinformation Review, 5 October 2022, https://doi.org/10.37016/mr-2020-107

[16] Despite proposals for an exemption for Public Interest Platforms presented by a coalition of organisations. For more information, see Wikimedia. Open call by UK civil society to exempt public interest projects from the Online Safety Bill. Available at: https://wikimedia.org.uk/2023/06/online-safety-bill-open-letter/

Question	Your response
	of YouTube's "rabbithole" qualities with regard to extremist content[17]; ● The degree of "polarisation" of content that average individual users or groups see on the platform; for example, Twitter's personalised timeline algorithm has been found to disproportionately amplify particular political opinions for particular users;[18] We believe these objective and measurable factors will be highly relevant for a system of service categorisation that accurately captures the differences between public interest platforms and commercial ad-revenue-driven platforms, which – even if the user numbers were the same – pose very different risks to users. Footnotes 15. Research ICT Africa, Digital Governance and the challenges for trust and safety. Part 1 (2023). Available at : https://researchictafrica.net/wp/wp-content/uploads/2023/02/Part-1-.pdf. Also see Carlos Carrasco-Farré, 'The Fingerprints of Misinformation: How Deceptive Content Differs from Reliable Sources in Terms of Cognitive Effort and Appeal to Emotions', Humanities and Social Sciences Communications 9, no. 1 (9 May 2022): 1–18, https://doi.org/10.1057/s41599-022-01174-9; Ullrich K. H. Ecker et al, 'The psychological drivers of misinformation belief and its resistance to correction', 2022, https://www.nature.com/articles/s44159-021-00006-y.pdf; Lan Ha, Timothy Graham, and Joanne Gray, 'Where Conspiracy Theories Flourish: A Study of YouTube Comments and Bill Gates Conspiracy Theories', Harvard Kennedy School Misinformation Review, 5 October 2022, https://doi.org/10.37016/mr-2020-107 16. Despite proposals for an exemption for Public Interest Platforms presented by a coalition of organisations. For more information, see Wikimedia. Open call by UK civil society to exempt public interest projects from the Online Safety Bill. Available at: https://wikimedia.org.uk/2023/06/online-safety-bill-open-letter/ 17. Kevin Roose, 'The Making of a YouTube Radical', The New York Times, sec. Technology (8 June 2019). Available at: https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html 18. Ferenc Huszár. Sofia Ira Ktena, Conor O'Brien, Luca Belli, Andrew Schlaikjer and Moritz Hardt, 'Algorithmic Amplification of Politics on Twitter'(2021). Available at: https://cdn.cms-twdigitalassets.com/content/dam/blog-twit

[17] Kevin Roose, 'The Making of a YouTube Radical', The New York Times, sec. Technology (8 June 2019). Available at: https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html

[18] Ferenc Huszár. Sofia Ira Ktena, Conor O'Brien, Luca Belli, Andrew Schlaikjer and Moritz Hardt, 'Algorithmic Amplification of Politics on Twitter'(2021). Available at: https://cdn.cms-twdigitalassets.com/content/dam/blog-twitter/official/en_us/company/2021/rml/Algorithmic-Amplification-of-Politics-on-Twitter.pdf

Question	Your response
	ter/official/en_us/company/2021/rml/Algorithmic-Amplification-of-Politics-on-Twitter.pdf
Question 9: Do you have evidence of factors that may affect how content that is illegal or harmful to children is disseminated on U2U services? ● **Are there particular functionalities that play a key role in enabling content that is illegal or harmful to children to be disseminated on U2U services?** ● **Do you have evidence relating to the relationship between user numbers, functionalities and how content that is illegal or harmful to children is disseminated on U2U services?**	Confidential – N In addition to the functionalities listed in response to question 6 (which apply to the dissemination of all content), there are some additional factors that may increase or reduce the dissemination of content which is illegal or harmful to children on U2U services. While we are not a U2U service and therefore do not have specific empirical evidence on the exact relationship between such factors and the dissemination of illegal or harmful content, factors that we believe should be included in for consideration in categorisations include: ● The reliability and accuracy of the U2U service's content moderation systems and processes, including human content reviewers as well as automated tools such as hashing or text and image processing (for commentary and recommendations, see our response to question 11 of Ofcom's first call for evidence[19] or our responses to questions 20-24 of Ofcom's second call for evidence[20]) ● The availability of simple, accessible and timely reporting mechanisms for suspicious, harmful or illegal content, including mechanisms which are child-friendly (see our response to question 7 of Ofcom's first call for evidence[21]; ● The use of alternative means of reducing the dissemination of harmful or illegal content such as counterspeech, re-direction and middleware/user controls (for a full list, see our response to question 18 of Ofcom's first call for evidence)[22] With regards to illegal content which is shared on private channels, at present there is little data on the degree to which the availability of encryption is a factor impacting the dissemination of content which is illegal or harmful to children. While encryption may facilitate or protect users from sharing illegal content without scrutiny, it remains an essential tool for protecting privacy and

[19] Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf
[20] Ofcom Call for Evidence: Second Phase of Online Safety Regulation Global Partners Digital Submission March 2023. Available at: https://gp-digital.org/wp-content/uploads/2023/06/GPD-Ofcom-submission-March-2023.pdf
[21] Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf
[22] Ibid.

Question	Your response
	safety in the online environment. As highlighted by countless organisations,[23] implementing measures that would compel online platforms to undermine encryption, such as requiring the use accredited technologies to scan content shared on private channels, infringes the privacy of users and undermines the security of the whole system, leaving it vulnerable to exploitation by malicious actors. Additional factors that are likely to impact the dissemination of content which is not illegal but which may be harmful to children include: ● The degree to which children and adult users are encouraged or facilitated to interact with one another on the service; ● The availability of default or stronger safety and privacy settings for children, which might prevent them from interacting with users who are not contacts or from viewing or sharing content outside of their friends lists; ● The availability of parental controls or "childsafe" modes or versions of a U2U service, or the implementation and enforcement of an age assurance system which limits child users from accessing age-inappropriate content; ● The degree to which children are encouraged to interact with content through recommendations or ranking algorithms based on their personal or behavioural data (see, for example, 5Rights Foundation's research on the amplification of content relating to dieting, self-harm, pornography and sexualised imagery based on children's interests and previous browsing history[24]). For a full list of recommendations on best practice with regards to addressing or limiting the dissemination of content which is illegal or harmful to children, please see our submission to Ofcom's call for call for evidence: second phase of online safety regulation (March 2023), including reducing the collection of children's personal data by U2U services for the purposes of targeting them with personalised content or ads, and providing children

[23] Online Safety Bill: Civil society organisations urge UK to protect global digital security and safeguard private communication. Available at: https://www.openrightsgroup.org/app/uploads/2023/06/Online-Safety-Bill-Civil-Society-Open-Letter-June-2023.pdf

[24] 5rights Foundation. Pathways: How digital design puts children at risk (July, 2021) Available at: https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

Question	Your response
	with tools to easily reject, block or report harmful or undesirable content. Footnotes: 19. Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf 20. Ofcom Call for Evidence: Second Phase of Online Safety Regulation Global Partners Digital Submission March 2023. Available at: https://gp-digital.org/wp-content/uploads/2023/06/GPD-Ofcom-submission-March-2023.pdf 21. Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf 22. Ibid. 23. Online Safety Bill: Civil society organisations urge UK to protect global digital security and safeguard private communication. Available at: https://www.openrightsgroup.org/app/uploads/2023/06/Online-Safety-Bill-Civil-Society-Open-Letter-June-2023.pdf 24. 5rights Foundation. Pathways: How digital design puts children at risk (July, 2021) Available at: https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
Question 10: Do you have evidence of other objective and measurable characteristics that may be relevant to category 2B threshold conditions?	Confidential – N As well as considering simply the number of users of a U2U service or the prevalence of certain content types on the service, category 2B threshold conditions could also draw upon: ● The number of child users of a service (N.B. research from 5Rights foundation indicates that 42% 5-12 year olds use social media apps and sites and 98% of young children over the age of 10 are online[25]) ● The proportion of revenue generated by ads specifically targeted at children; ● The number of reports of content which is harmful to children made by users, and the proportion of such reports found to be accurate upon review; ● The number of child users that viewed content later removed as age-inappropriate or illegal; ● Objective and measurable data capturing user experiences and opinions, such as the degree to which child users or their guardians perceive

[25] Ibid.

Question	Your response
	their experience to be affected or impacted by the presence of particular content types or wish for more or less content moderation interventions. For example, a survey conducted by Pew Research Centre in 2022 explored American teens' opinions on the benefits and downfalls of large U2U services.[26] While 23% reported that large U2U services could make them feel "worse about their life", only 9% said that its impact on their lives had been "mostly negative" and more than 30% said that its effect had been "mostly positive". Footnotes 25. Ibid. 26. Pew Research Center. Teens and social media: Key findings from Pew Research Center surveys (24 April, 2023). Available at: https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/
Question 11: Do you have evidence of matters that affect the prevalence of content that (once the Bill takes effect) will count as search content that is illegal or harmful to children on particular search services or types of search service? For example, prevalence could refer to the proportion of content surfaced against each search term 16 that is illegal or harmful to children, but we welcome suggestions on additional definitions. ● **Do you have evidence relating to the measurement of the prevalence of content that is illegal or harmful to children on search services?**	Confidential – N The prevalence of content that is illegal or harmful to children on particular search services or types of search service will depend on a number of factors. While we are not a search service and therefore cannot provide empirical data, we would encourage Ofcom to consider the following factors in its categorisation decisions: ● The degree to which a search service's ranking algorithm (e.g. Google's Page Rank) prioritises content from reputable or reliable sources earlier in its page results, rather than simply presenting content which is most likely to generate clicks; ● The reliability and accuracy of the search service's content moderation systems and processes, including human content reviewers as well as automated tools such as hashing or text and image processing, which identify and de-rank or de-index illegal and/or harmful content; ● The availability of simple, accessible and timely reporting mechanisms for suspicious, harmful or illegal content, including mechanisms which are

[26] Pew Research Center. Teens and social media: Key findings from Pew Research Center surveys (24 April, 2023). Available at: https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/

Question	Your response
	child-friendly (see our response to question 7 of Ofcom's first call for evidence[27]; ● The availability of "child-safe" modes or different settings which allow users or parents to filter or block undesirable content types; ● The use of alternative means of reducing the prevalence and visibility of harmful or illegal content such as counterspeech, re-direction and middleware/user controls (for a full list, see our response to question 18 of Ofcom's first call for evidence).[28] Footnotes: 27. Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf 28. Ibid.
Question 12: Do you have evidence relating to the number of users on search services and the level of risk of harm to individuals from search content that is illegal or harmful to children? ● **Do you have evidence regarding the relationship between user numbers on search services and the prevalence of search content that is illegal or harmful to children?**	Confidential – N While we are not a search engine and therefore are not able to draw on our own empirical evidence, large search services have more users and therefore if there is harmful content being ranked high up, more people will see it -- but conversely, they also have much larger budgets, content moderation systems, and incentives to provide recommendations of content that can be perceived as quality content by they users to keep them engaged. Therefore, the likelihood of illegal content or harmful to children being left up for users to experience is lower. Conversely, there can be search services with a relatively small base of users that can offer niche service with a higher likelihood of lacking the quality control and moderation features that could prevent the contact with illegal content or harmful to children.
Question 13: Do you have evidence of other objective and measurable characteristics that may be relevant to category 2A threshold conditions?	Confidential – N As with U2U services, many search engines are driven by a business model reliant upon retaining user attention to generate advertising revenue, and commonly use micro-targeting and automated, personalised advertising

[27] Ofcom Call for Evidence: First Phase of Online Safety Regulation Global Partners Digital submission September 2022. Available at: https://gp-digital.org/wp-content/uploads/2022/09/Ofcom-Call-for-Evidence-.pdf
[28] Ibid.

Question	Your response
	systems for maximum click-throughs.[29] While we are not a search engine and therefore are not able to draw on our own empirical evidence, we encourage Ofcom to consider the following factors and characteristics in determining whether a search engine should be subject to additional scrutiny as a 2A platform; ● The amount of personal data collected by the search service, for example the number of data points, characteristics or behaviours that are used to inform the search service's ranking algorithm and ad targeting system; ● The proportion of service revenue that is generated by ad placements; ● The number of children using the search service; ● The use of share buttons, sometimes functioning as nudges or dark patterns[30] prompting users to share, repost or take some other action in relation to a webpage surfaced in search results; ● Functionalities which encourage or facilitate "virality" of timely or trending content, promoting results relating to a particular topic or event more prominently in the ranking algorithm or using hashtags, alerts or labels to index relevant content. Footnotes: 29. Research ICT Africa, Digital Governance and the challenges for trust and safety. Part 1 (2023). Available at : https://researchictafrica.net/wp/wp-content/uploads/2023/02/Part-1-.pdf. Also see Carlos Carrasco-Farré, 'The Fingerprints of Misinformation: How Deceptive Content Differs from Reliable Sources in Terms of Cognitive Effort and Appeal to Emotions', Humanities and Social Sciences Communications 9, no. 1 (9 May 2022): 1–18, https://doi.org/10.1057/s41599-022-01174-9; Ullrich K. H. Ecker et al, 'The psychological drivers of misinformation belief and its resistance to correction', 2022, https://www.nature.com/articles/s44159-021-00006-y.pdf;

[29] Research ICT Africa, Digital Governance and the challenges for trust and safety. Part 1 (2023). Available at : https://researchictafrica.net/wp/wp-content/uploads/2023/02/Part-1-.pdf. Also see Carlos Carrasco-Farré, 'The Fingerprints of Misinformation: How Deceptive Content Differs from Reliable Sources in Terms of Cognitive Effort and Appeal to Emotions', Humanities and Social Sciences Communications 9, no. 1 (9 May 2022): 1–18, https://doi.org/10.1057/s41599-022-01174-9; Ullrich K. H. Ecker et al, 'The psychological drivers of misinformation belief and its resistance to correction', 2022, https://www.nature.com/articles/s44159-021-00006-y.pdf; Lan Ha, Timothy Graham, and Joanne Gray, 'Where Conspiracy Theories Flourish: A Study of YouTube Comments

[30] Dark patterns often take advantage of consumers' cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions. For more information, see Federal Trade Commission. Bringing Dark Patterns to Light (2022). Available at: https://www.ftc.gov/reports/bringing-dark-patterns-light; European Data Protection Board. Guidelines on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 (2023). Available at: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdfand Bill Gates Conspiracy Theories', Harvard Kennedy School Misinformation Review, 5 October 2022, https://doi.org/10.37016/mr-2020-107

Question	Your response
	Lan Ha, Timothy Graham, and Joanne Gray, 'Where Conspiracy Theories Flourish: A Study of YouTube Comments 30. Dark patterns often take advantage of consumers' cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions. For more information, see Federal Trade Commission. Bringing Dark Patterns to Light (2022). Available at: https://www.ftc.gov/reports/bringing-dark-patterns-light; European Data Protection Board. Guidelines on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 (2023). Available at: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdfand Bill Gates Conspiracy Theories', Harvard Kennedy School Misinformation Review, 5 October 2022, https://doi.org/10.37016/mr-2020-107

Please complete this form in full and return to os-cfe@ofcom.org.uk.