23 February 2024

Ofcom Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

By email to: IHconsultation@ofcom.org.uk

RESPONSE TO CONSULTATION ON PROTECTING PEOPLE FROM ILLEGAL HARMS ONLINE UNDER THE ONLINE SAFETY ACT 2023

1. This is the response of Mega Limited (**Mega**) to Ofcom's consultation on protecting people from illegal harms online under the Online Safety Act 2023 (the **Consultation**).

Mega Limited

2. Mega is an end-to-end encrypted cloud storage and communication services provider, with 300 million registered user accounts in 250 countries and territories, who have uploaded more than 150 billion files.

3. Mega operates globally from its head office in Auckland, New Zealand. Mega has extensive experience with requests for information from international authorities, together with actioning reports of illegal or objectionable activity from both international authorities and other reporters.

4. Our brand by-line is **The Privacy Company**, because we offer end-to-end encrypted cloud storage and communication services, and privacy is a core value going to the heart of everything we do. Our users value being able to store data in a manner that is not vulnerable to third party attack on our servers and which cannot be scraped or stolen by advertisers or other third parties. Some users, such as journalists and minority groups based in countries with oppressive regimes, value having added protection from Government surveillance.

5. Files or data uploaded to our servers are encrypted at the user's device and cannot be reviewed by us (or anyone) unless we or they are provided with an encryption key which is known only to the user and anyone they choose to share it with. Users can generate unique URLs/links to their stored files which include encryption keys and, when shared, will allow third parties to decrypt, access, view and download the relevant content.

6. Unfortunately, like all OSPs, a small proportion of our users use our services for unlawful purposes. Mega has zero tolerance for such conduct and is widely commended by both local and international law enforcement agencies in regards to its compliance and disclosure processes.

7. We are proud of the steps we have taken to respond to unlawful or improper use of our services. We regularly publish Transparency Reports which detail the actions we have taken. All of these reports, including our most recent for the six months to 30 September 2023 can be viewed at https://mega.io/transparency.

8. Mega is a member of the Tech Coalition, the Global Internet Forum to Counter Terrorism (**GIFCT**), the Christchurch Call community, WeProtect Global Alliance and the Asia-Pacific Financial Coalition Against Child Sexual Exploitation (**APFC**). Mega is actively involved in industry initiatives to combat unlawful activity online and is aware of current industry trends and standards in this regard. For example, Mega actively participates in Lantern, the first cross-platform signal sharing for companies to strengthen how they enforce their child safety policies.[1]

9. In view of the above, we consider we are well placed to respond to the Consultation and set out our comments below. We have not answered the specific questions set out in the consultation response form but have instead reviewed the summary of Ofcom's proposals and summary of each chapter and certain parts of Volumes 1 – 6 and Annexes 1-16.

10. It is regrettable that the size of the Consultation (over 1,700 pages of documentation and 55 questions in total) means that only very large businesses will have the resources necessary to meaningfully and comprehensively respond to the Consultation. Volume 3 and Annex 5 on risk assessment alone, the key issue in this Consultation, are 167 pages. We have found this level of volume and complexity counterproductive. It made it difficult to understand the guidance provided in the Consultation.

11. Considering the size of the Consultation and the time available to us during the New Zealand summer, we have only been able to comment at a very high level on a limited number of specific points as they pertain to smaller services like Mega – our not commenting on any topic or not responding to the questions in the consultation response form is not an indication that we agree with or have no views on the subject-matter of any given topic or question.

Our comments

High-level comment

12. Mega's main concern is that the guidance and measures proposed by Ofcom under the OSA in the Consultation are incredibly complex to comprehend and will be overly cumbersome to implement. It **must** be simplified. Ofcom's objective under the OSA appears to have been to design a 'perfect' 'all-encompassing' system that would regulate every aspect of an online service's life relating to online safety. In our view this has led to a guidance and measures that are unworkable and that will too often be impossible to implement. Instead, the approach should have been targeted in a manner proportionate to the harm caused as well as to the relevant platform involved.

13. The best corporate citizens, like Mega, will do their best to follow and apply such complex, expensive guidance and measures. The measures will, however, be ignored by the worst actors. This means that good corporate citizens will encounter significant difficulties, while

[1] See https://www.technologycoalition.org/newsroom/announcing-lantern for more information about Lantern.

the broader online safety problems sought to be addressed will not be properly resolved. The emphasis in the Consultation should have been on specifically targeting the worst unsatisfactory platforms (which are already well known).

14. This could be achieved by having simpler to achieve yet specific, measurable, relevant and time-bound guidance and measures and by putting on notice those specified platforms of their deficiencies and proven poor performance in dealing with known harms. By contrast, platforms that are currently acting appropriately and who intend to comply with the OSA as best they can would not face incurring the significant resources and costs involved in adhering to the complex and burdensome guidance and measures set out in the Consultation.

End-to-end encryption

15. Mega was pleased to read in the Consultation that Ofcom considers that "the role of new online safety regulation is not to restrict or prohibit the use of [end-to-end encryption]"[2] and that "[Ofcom's] measures would not apply to services that are technically unable to analyse user-generated content present or disseminated on the service to assess whether it is content of a particular kind, particularly where such changes as would need to be made to enable this would materially compromise the security of the service. For example, we acknowledge that end-to-end encrypted services are currently unable to analyse user-generated content in the ways set out in our proposals."[3]

16. However, Ofcom also states in the Consultation that:

(a) "[end-to-end encryption (**E2EE**) is a functionality] that stands out as posing a particular risk";[4]

(b) "encryption and ephemerality make messaging particularly attractive to terrorist actors as they can reduce the chance of detection";[5] and

(c) "end-to-end encryption can enable perpetrators to circulate CSAM, engage in fraud, and spread terrorist content with a reduced risk of detection".[6]

17. Consistently with s 9(5)(c) of the OSA, Ofcom considers that the particular risk posed by E2EE is not only about content itself but also about how E2EE services are used by criminals, and more specifically that when assessing the risk of online harm on their services, user-to-user (**U2U**) services need to consider the risk of "an offence being committed using the services" or of "an offence being facilitated by use of the service".[7]

18. Our view is that smaller services cannot be expected to be able to assess whether they are being used for the commission or facilitation of many of the priority offences that are not image-based, such as fraud, financial services offences or proceeds of crime. To do so, relevant content (typically text-based) would need to be carefully reviewed and analysed. Unlike reviewing content relating to image-based offences such as CSAM or violent

[2] Protecting people from illegal harms online – Summary of Each Chapter, page 9
[3] Protecting people from illegal harms online - Volume 4; 14.16, page 94
[4] Protecting people from illegal harms online – Summary of Each Chapter, page 8
[5] Protecting people from illegal harms online - Volume 2: the causes and impacts of online harm; page 32
[6] Protecting people from illegal harms online - Volume 2: the causes and impacts of online harm; page 3
[7] Annex 5, Draft Service Risk Assessment Guidance; A5.23, page 7

extremism, this requires investigative work which smaller services are not equipped to undertake. Larger services may also have the same problem.

19. Further (and significant) complexity arises from jurisdictional issues and the different criminal laws applying to users all around the world, in circumstances where the location of any given user is not always clear. Smaller services, in particular those based outside of the UK, cannot be expected to have the resources and expertise to know and interpret UK criminal law relating to all 130 priority offences set out in the Consultation. Whilst Mega appreciates that (a) it is inevitable that any law regulating online activities will have some extraterritorial effect and (b) certain kinds of image-based harms are easily identified regardless of which country's criminal law applies, Ofcom's approach to risk assessment imposes an unreasonable and disproportionate burden on smaller services. It goes much further than assessing whether illegal content (typically image-based content) is present on the service or taking prompt action when such content has been identified (which Mega infallibly does).

20. By way of example, prostitution is not a crime in New Zealand. Holding Mega liable because its E2EE U2U services were used to facilitate prostitution in the United Kingdom or because it failed to properly assess the risk of such "harm" under the OSA is a bridge too far in Mega's view. Treatment of controlled drugs also varies widely in different jurisdictions.

21. Ultimately, E2EE U2U services are mere conduits of content. Mega cannot, nor does it wish to, use recommender services or artificial intelligence (**AI**). E2EE simply makes it impossible. This is because the data stored and messages exchanged on E2EE U2U services cannot be analysed by, or used to train, an AI or an algorithm. When encrypted, files and messages are just indecipherable blobs of data. It also means that objectionable or illegal content will not be proactively distributed or displayed to users in accordance with algorithms or otherwise by E2EE U2U services. For example, in Mega's case, a URL can be created by a user to share data publicly (the decryption key being embedded in the URL) but the URL must then be sent via emails or some other online services to reach a large audience. On Mega Chat, a user cannot usually be messaged by, let alone receive files from, someone who is not in their contacts list. This could only happen when a user willingly participates in a public chat on which they can easily block any use and which they can easy leave at any moment. This is in fact Enhanced User Control by default.

22. Under the Service Risk Assessment Guidance, it tentatively appears that Mega would qualify as a multi-risk smaller service (although we express no view on this at this stage). This is despite the fact that, for the reasons set out above, E2EE creates a very specific kind of risk, mainly content risk inherent to its zero-knowledge nature. By contrast, a service (smaller or large) that uses AI, recommender services and no Enhanced User Control features will create a much wider variety of risks. Yet, Ofcom intends to impose a near identical level of obligations on smaller multi-risk services and large multi-risk services.[8] This is unreasonable.

Categorisation of services

23. While we can see benefit in breaking down the "smaller" and "large" service categories in order to apply less onerous obligations on services that are lower risk, the distinctions between "low risk", "specific risk", and "multi-risk" do not seem to be sensible. We have difficulty conceiving of any online service that would be medium or high risk for only one of

[8] See table 1 of "Consultation at a glance".

the 15 priority harms, but none of the others. This makes the “specific risk” category largely redundant from our perspective.

24. It is also concerning that multi-risk smaller services are proposed to be subject to the majority of measures that would apply to large services. While Ofcom has acknowledged the resource limitations applying to smaller services, that is not reflected in the proposed measures – any flexibility that might have been afforded to a smaller service is effectively stripped away as soon as that service identifies it has a medium or high risk of only two illegal harms.

25. It follows that the breakdown of services and distinctions between them seem to us to be fairly illusory. They should either be re-cast in a more practical and realistic fashion (our preference), or discarded.

Governance & Accountability

26. Mega would like to take comfort in Ofcom’s statement that “we will flex our expectations depending on the type of service we are dealing with”, “not taking a one-size-fits all approach”.[9]

27. However, in line with our comment at paragraph 22 above, it appears to us that measures like imposing a Code of Conduct[10] for all staff are overly burdensome to smaller services who mainly deal with image-based illegal/objectionable content. This is despite the fact that Ofcom acknowledges in the Consultation that “larger services will tend to be better able to bear the costs of the more onerous measures than smaller services”.[11]

28. Some of the measures proposed for U2U services in table 1 of the ‘Consultation at a glance’ document ignore the reality of running a business. For example, proposed measures 3B, 3C, 3D, 3E and 3G are just normal business operations for good corporate citizens; businesses have management structures, responsibilities and accountabilities. Documenting such operations for the specific purpose of complying with the guidance and measures proposed by Ofcom is overly bureaucratic and resource intensive for little practical benefit.

Reviewing content

29. In the Consultation, Ofcom states that services should “prepare and apply a policy about the prioritisation of content for review”[12] and proposes measure 4D whereby “when prioritising what content to review, regard is had to the following: […] potential severity of content and the likelihood that content is illegal”. It is simply impossible to assess those factors and prioritise without first reviewing the content.

30. Proposed measure 5C will also likely become counterproductive. Whatever ‘indicative’ timeframe is communicated, users will complain if their response is delayed beyond that time, so it is an incentive for platforms to specify a much longer timeframe than would typically be achieved.

[9] Protecting people from illegal harms online – Summary of Each Chapter, page 6
[10] See Consultation at a Glance; reference 3F, page 3
[11] Protecting people from illegal harms online – Summary of Each Chapter, page 16
[12] Protecting people from illegal harms online – Summary of Each Chapter, page 17

User access - terrorism

31. Under proposed measure 10A, accounts should be removed if there are reasonable grounds to infer they are run by or on behalf of a terrorist group or organisation proscribed by the UK Government. Our view is that this should be done by reference to internationally accepted standards/lists, such as the United Nations Security Council Consolidated List.

Concluding remarks

32. As can be seen from the above high-level remarks, we have significant concerns with this proposal. We appreciate that Ofcom has been open to feedback and we hope that this consultation process will result in significant and meaningful changes. We would be happy to speak to, or expand on, any of the above response.

MEGA THE PRIVACY COMPANY