21 December 2023

Office of the eSafety Commissioner
Industry Regulation and Legal Services
Executive Manager,
PO Box Q500, Queen Victoria Building
NSW 1230

By email to: submissions@esafety.gov.au

SUBMISSION BY MEGA LIMITED ON THE DRAFT ONLINE SAFETY (DESIGNATED INTERNET SERVICES – CLASS 1A AND 1B MATERIAL) INDUSTRY STANDARD 2024

1. This submission is made on behalf of Mega Limited (**Mega**) in response to the eSafety Commissioner's draft Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024 (**the Draft Standard**).

Mega Limited

2. Mega is the largest New Zealand-based Online Service Provider (**OSP**). We have over 296 million registered users around the world. Similarweb currently ranks our site, mega.nz, as the 283rd most visited site in the world. Dropbox and MEGA are ranked 2nd and 3rd respectively in the category of sites providing file sharing and hosting.

3. 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.

4. 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.

5. Unfortunately, like all OSPs, a small proportion of our users use our services for unlawful purposes. Mega has zero tolerance for such conduct. 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.

6. 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**). We are actively involved in

industry initiatives to combat unlawful activity online and are aware of current industry trends and standards in this regard.

7. [redacted]

8. In view of the above, we consider we are well placed to provide you with feedback concerning the Draft Standard. We have not answered the specific questions set out in the Discussion Paper but have instead reviewed the Draft Standard on a section-by-section basis. We set out our below our comments on some sections of the Draft Standard. In the time available we have only been able to comment on some key issues – our not commenting on any given section or not responding to the questions is not an indication that we agree with or have no views on the subject-matter of any given section or question.

Our comments

9. Mega welcomes the Commissioner's clear statements to the effect that the Draft Standard does not require encryption to be weakened or subverted, and that alternative technical means may be identified for encrypted services to detect or respond to CSAM and/or pro-terror material.[1]

10. We protect the privacy of our legitimate users but we have zero tolerance for unlawful or harmful content being stored or shared by other users. As a result, and notwithstanding the end-to-end encryption which is fundamental to our service, Mega has developed a number of industry-leading methods for responding to the content that is reported to us. This is outlined in more detail in our transparency reports.

Use of certain defined terms in the Draft Standard

Child sexual exploitation material, pro-terror material, Class 1A and Class 1B material

11. The Draft Standard defines 'class 1A material' but does not appear to take full advantage of that defined term.

12. It makes the Draft Standard harder to follow if the three types of materials included in the definition of class 1A material (CSEM, pro-terror material and extreme crime and violence material) are used separately such that different obligations apply in relation to some of them as is currently the case across ss 15 and 17 (which deal with CSEM and pro-terror material but not extreme crime and violence material), s19 (which deal with extreme crime and violence material and class 1B material) and s 23 (which also deal with CSEM and pro-terror material but not extreme crime and violence material).

[1] eSafety Commissioner, *Discussion paper – Draft Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 and Draft Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024* (November 2023), pp 12-14.

13. It seems to us it would be preferable to use the term 'class 1A material' in ss 15, 17 and 23 so as to cover all three types of material included in the definition of class 1A material. We see no reason to exclude extreme crime and violence material from s 15.

14. With the above changes, extreme crime and violence material would not need to be covered by s 19 and references thereto should be deleted. This would overall simplify Part 4 of the Draft Standard.

Known CSAM and known pro-terror material

15. You have asked whether the technical feasibility exception in the obligation to detect and remove known child sexual abuse material and pro-terror material is appropriate, and how effective will this obligation be with this exception. As noted above, we support allowing services which are end-to-end encrypted the ability to use other technical means of dealing with illegal content, and we have found that there are a number of such means available.

16. [redacted]

17. [redacted]

18. A Designated Internet Services (**DIS**) would need to expend an untenable level of resources to comprehensively establish that material is or is not known CSAM or pro-terror. We say more below on why the obligations set out at ss 21 and 22 to detect and remove known CSAM and known pro-terror material should be subject to a proportionality test by reference to the defined term 'appropriate action'.

19. In addition, automatic application of such technology as mandated by ss 21(8) will likely lead to many false positive results. Section 21(8) should be deleted in our view.

'Community standards'

20. The term 'community standards' is used several times in the Draft Standard (in ss 12, 16, 17, 18, 19, 25 and 32.).

21. We understand 'community standards' to mean the rules and guidance issued by any given DIS on what is and what is not acceptable to post on the service. However, the term is not defined in the Draft Standard. Mega's view is that use of the term, as undefined, may lead to confusion as to whether it means the standards used by each platform, or 'community standards' in the general community. In addition, Mega does not publish 'community standards'. Usage restrictions are specified in Mega's Terms of Service and its Takedown Guidance Policy.

22. For clarity, 'community standard' should be:

(a) Defined, as above, and included in the definition of 'terms of use' at s 6 of the Draft Standard;

(b) Deleted from the rest of the Draft Standard (subject to the below exception) as it will become redundant. In particular, ss 16(2)(b), 17(2)(b), 18(2)(b) and 19(2)(b) should be deleted. We see no advantage to distinguishing between "a breach of an obligation under the terms of use for the service" and "a breach involving the service of community standards"; and

(c) Retained in s 32(2)(b) and the words 'if any' should be added at the end of that subsection.

Part 3

23. Section 8(6) provides that ss 8(1) and 8(4) do not apply to end-user managed hosting services. The flow on effect is that none of Part 3 applies to end-user managed hosting services.

24. For clarity, the Draft Standard should make it expressly clear that the whole of Part 3, not just ss 8(1) and 8(4), does not apply to end-user managed hosting services.

Section 14(2)

25. Section 14(2)(a) provides that a DIS "must include provisions in the terms of use of the service which impose an obligation on the account holder of the service which to ensure that the service is not used .... to solicit, access, ... class 1A material or class 1B material..."

26. The mere presence of such an obligation cannot 'ensure' that the service will not be used for the contemplated illegal purpose. The obligation on the provider should be to include such an obligation in its terms of use (and to enforce it); not that the obligation ensures a specific goal.

27. To that end, Mega suggests changes to s 14(2)(a) as shown in redline below:

> (2) The provider of a service must include provisions in the terms of use for the service that:
>
> (a) impose an obligation on the account holder of the service ~~to ensure that the service is~~ not to use the service~~d~~, whether by the account holder or an end-user[2] in Australia, to solicit, access, generate, distribute or store (as applicable, having regard to the purpose and functionality of the service) class 1A material or class 1B material; and

Section 14(3)

28. In light of the definition of 'appropriate action' at s 12 (which includes a proportionality test) we suggest the wording of s 14(3) can be simplified as shown below:

> (3) If the provider of a service becomes aware of a breach of the obligation mentioned in subsection (2)(a), the provider must take appropriate action to enforce its contractual rights in respect of the breach ~~in an appropriate way that is proportionate to the extent of the harm to the online safety of Australians that may reasonably be expected to flow from the breach~~.

Evidential burden under s 14(4)

29. We disagree that in proceedings in respect of a contravention of subsection (3), the provider should bear the evidential burden of establishing the action it took to enforce the rights and that the action that it took was appropriate and proportionate, as set out in s 14(4).

30. This shifting of the evidential burden is inconsistent with well-established principles of natural justice. Section 14(4) should be deleted.

'Further such breaches' at ss 16(2)(d)[2], 17(3)(c) and 18(2)(d)

31. It is not clear to us what is meant by 'further such breaches' at ss 16(2)(d)[3], 17(3)(c) and 18(2)(d). These subsections should only impose duties to take appropriate action to ensure the risk that the same user will commit the same type of breach is minimised, not impose much broader duties to take action to ensure the risk that other users will commit the same type of breach is minimised. Mega's view is that the latter interpretation is much too broad (and redundant with / cutting across other parts of the Draft Standard) such that the former interpretation makes more sense. This should be clarified in the Draft Standard.

Section 17(2)(c)

32. In many cases CSEM or pro-terror material is taken down before an enforcement authority gets involved. In our experience, law enforcement agencies often approach service providers to obtain evidential material months or even years after content was taken down. Providers should have the option to securely preserve the instances of CSEM and pro-terror material for law enforcement purposes rather than have it removed from their service. We suggest amending subsection 17(2)(c) as follows:

> the provider must:
>
> (c) remove public access to instances of CSEM and pro-terror materials identified by the provider on the service as soon as reasonably practicable and may securely preserve those instances as evidence for potential future investigation and/or prosecution purposes without incurring liability unless otherwise required to deal with unlawful CSEM and pro-terror materials by an enforcement authority;

Section 17(2)(d)

33. In light of the definition of 'account holder' and 'end-user' in s 6 of the Draft Standard, 'the account' referred to in s 17(2)(d) cannot be the end user's but should be the account holder's. We suggest amending s 17(2)(d) as shown further below.

34. The rest of s 17(2)(d), subsections 17(2)(d)(i)-(iii) are superfluous in our view. If an account is linked to CSEM or pro-terror material in breach of terms of use, it should be terminated (subject to any valid appeal by the affected user). There should not be any further considerations: for example there should not be a requirement that the CSEM or pro-terror material be distributed to end-users "with the intention to cause harm" as set out at subsection (2)(d)(i). A service provider is very unlikely to be able to judge whether there was an intention to harm anyway.

35. In other words, a breach of an obligation under the terms of use for the service in respect of CSEM or pro-terror material is in itself sufficient to justify terminating an account, regardless of whether:

(a) It is distributed with the intention to cause harm as set out at subsection (2)(d)(i);

(b) it involves an Australian child using the account as set out at subsection (2)(d)(ii); or

(c) the breach is repeated or not, as set out at subsection (2)(d)(iii).

[2] We note s 16(2)(d) is numbered 16(2)(b) in error on page 22.
[3] We note s 16(2)(d) is numbered 16(2)(b) in error on page 22.

36. We suggest s 17(2)(d) should read:

> (c) terminate ~~an end-user's~~the account used by the end-user as soon as reasonably practicable ~~if the end-user:~~
>
> ~~(i) is distributing CSEM or pro-terror materials to end-users with the intention to cause harm;~~
>
> ~~(ii) is known to be an Australian child using the account; or~~
>
> ~~(iii) has repeatedly breached terms and conditions, community standards or acceptable use policies prohibiting CSEM and pro-terror materials on the service.~~

Sections 21 and 22

Detecting and identifying known CSAM and pro-terror material

37. [redacted] the obligations set out at ss 21 and 22 should be subject to a proportionality test. We suggest amending the first sentence of ss 21(2) and 22(2) as follows:

> "The provider of a service must take appropriate action to implement systems, processes, and technologies that detect and identify..."

Consistency of language

38. Sections 21(2)(c) and 22(2)(c) use inconsistent language. Section 21(2)(c) refers to "instances of known CSAM that is being or has been accessed or distributed in Australia using the service" whereas s 22(2)(c) refers to "known pro-terror material that is being or has been generated, accessed or distributed in Australia using the service".

39. Section 22(4) refers to "instances of known pro-terror material".

40. For clarity and consistency:

(a) s 21(2) should refer to known CSAM rather than "instances of known CSAM";

(b) 'generated' should be added to s 21(2)(c) or removed from 22(2)(c); and

(c) s 22(4) should refer to known pro-terror material rather than "instances of known pro-terror material".

Section 23

41. The obligations set out at s 23 should also be subject to a proportionality test. We suggest amending s 23 as follows:

> (2) The provider of a service must take appropriate action to implement systems, processes and technologies that:
>
> (a) effectively deter end-users of the service from using the service; and
>
> (b) effectively disrupt attempts by end-users of the service to use the service;
>
> to solicit, generate, access, distribute, store or otherwise make available CSAM and pro-terror material (including known CSAM and known pro-terror material).

Section 24

42. Our view is that a development program should also be subject to a proportionality and appropriateness test and suggest adding wording to that effect as shown below:

(4) A development program must include, subject to proportionality and appropriateness:

(a) investments and activities designed to develop systems, processes and technologies that enhance the ability of the provider, or of other providers of designated internet services:

(i) to detect and identify child sexual abuse material or pro-terror material (including known child sexual abuse material and known pro-terror material) on the service; and

(ii) effectively to deter end-users of the service from using the service, and to disrupt attempts by end-users of the service to use the service, to generate, access, distribute or store child sexual abuse material or pro-terror material (including known child sexual abuse material and known pro-terror material); and

(b) arrangements for cooperating and collaborating with other organisations in activities of the kind referred to in paragraph (a) and to enhance online safety for Australians.

Section 28

43. The requirement that the information set out in s 28(2) be located 'in service' is unrealistic in our view. A link to a separate webpage, in particular in the case of a mobile application where there is very limited space to provide information in a user-friendly manner, should be acceptable, as similar requirements might be imposed by other jurisdictions, resulting in a length exposition of detailed information.

44. We suggest the last sentence of s 28(2) be deleted.

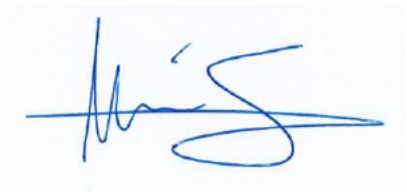
Section 34

45. Despite that fact that s 34(1) provides that s 34 applies to all DIS, ss 34(2)(a)–(c) do not apply to end-user managed services. This is because end-user managed services are not required to conduct a risk assessment to determine their risk profile under Part 3. It should be made clear in the Draft Standard that ss 34(2)(a)–(c) do not apply to end-user managed services.

Additional information eSafety should consider

46. As a general proposition, we would urge you to consider the obligations being imposed on DISs in different jurisdictions around the world, and ensure consistency as far as possible. Significant complexity, double-handling and complication can be introduced where countries take differing approaches to achieving the same overall goals. We are a small provider and we commit as much resource as we can to ensuring we comply with legislation and regulations applying to us worldwide, but complexity and variations across jurisdictions can cause us seemingly unnecessary cost and difficulty. We trust that you will take this into account in developing these standards.

Yours sincerely



Sébastien Aymeric – General Counsel
MEGA THE PRIVACY COMPANY

Mega Limited - +64 9 281 2110
Level 21, 120 Albert Street, Auckland
Private Bag 92533, Victoria Street West, Auckland 1142 - New Zealand
https://mega.nz