21 June 2024

Director – Strategy and Research
Online Safety, Media and Platforms Division
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601
AUSTRALIA

By email: OSAReview@COMMUNICATIONS.gov.au

RESPONSE TO ISSUES PAPER – STATUTORY REVIEW OF THE ONLINE SAFETY ACT 2021

1. This is the response of Mega Limited (**Mega**) to the 29 April 2024 Issues Paper – Statutory Review of the Online Safety Act 2021 (**Issues Paper**).

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 (**E2EE**) 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 Online Service Providers (**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. We are strong supporters of online safety, which we do not see as being inconsistent with our E2EE services, as we explain below.

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 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. We provide here some high-level responses to some of the questions contained in the Issues Paper, in the hope they will be of assistance to your review. Our not commenting on any topic or not responding to the questions in the Issues Paper is not an indication that we agree with or have no views on the subject-matter of any given topic or question.

Part 2 – Australia's regulatory approach to online services, systems and processes

4 – Should the Act have strengthened and enforceable Basic Online Safety Expectations?

10. We explain in more detail below our view that the Online Safety Act should, as far as possible, be technology neutral and sufficiently high level to allow adaptability for OSPs depending on their nature, user base, reach, and resources. That being so, it is our view that basic online safety expectations should be exactly that: basic and flexible, affording OSPs scope to find appropriate ways to meet those expectations.

5 – Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?

11. MEGA falls within the category of Designated Internet Services under the Act. As you will be aware, the eSafety Commissioner decided not to register the draft Standard for those services, and advised that a Standard would be determined by her. This was over a year ago and, as at the time of preparing these submissions, no Standard has yet been determined or registered.[2] That being so, it seems to us premature to comment on the drafting process or how it could be improved.

12. We note that the approach in the UK is not to mandate compliance with the Codes that are under development by Ofcom – services will be permitted to find other ways to meet their obligations under the UK Act if preferred. We commend the flexibility of that approach.

6 – To what extent should online safety be managed through a service provider's terms of use?

13. MEGA's terms of service (https://mega.io/terms) set out our expectations for our users in terms of how they use our services. All users are required to comply with all applicable laws, regulations and rules when using our services and with respect to any data they upload, access or share using our services. We also prohibit, for example, using our service to:

    13.1 Send unwelcome communications of any kind;

    13.2 Abuse, defame, threaten, stalk or harass anyone, or to harm them as defined in the Harmful Digital Communications Act 2015 (NZ) or any similar law in the relevant jurisdiction;

[1] See https://www.technologycoalition.org/newsroom/announcing-lantern for more information about Lantern.
[2] A new Standard appears to have just now been published (on 21 June 2024) – we have not yet reviewed this.

13.3 Store, use, download, upload, share, access, transmit, or otherwise make available, unsuitable, offensive, obscene or discriminatory information of any kind.

14. If a user breaches our terms of service, we are entitled to terminate their account without notice. We are also entitled to terminate their account if they provide us with information indicating they have breached or intend to breach our terms, or if we receive a credible report that a user has used another online service provider to do any of the things listed at [13.1]-[13.3] above. We can and do rely on these provisions to terminate user accounts every day (for more detail, see our transparency reports).

15. We see significant benefits in using our terms of service to manage online safety. In particular, our terms are cross-jurisdictional: they apply to all of our users, irrespective of where in the world they are located. This enhances and streamlines our internal processes and protocols as it limits situations in which we would need to take different approaches depending on the country of the user (which in any event may not be certain).

16. We aim to ensure our terms prohibit a broad range of conduct that we expect all (or the vast majority of) jurisdictions would consider harmful. Difficulty arises where, as in the United Kingdom (with the Online Safety Act), OSPs are expected to address specific criminal offences in specific jurisdictions. Smaller services cannot be expected to have the resources and expertise to know and interpret the precise crimes specified by the criminal law of every jurisdiction worldwide. 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, too much local specificity imposes an unreasonable and disproportionate burden on smaller services.

17. By way of example, prostitution is not a crime in New Zealand, but is one of the offences in the UK that the UK Online Safety Act provides must be identified and assessed in order that the risks of harm to individuals can be "effectively mitigated and managed". Holding MEGA liable because its services were used to facilitate prostitution in another jurisdiction or because it failed to properly assess the risk of such "harm" is a bridge too far in our view. Treatment of controlled drugs also varies widely in different jurisdictions. In our view, it is significantly preferable to rely on our terms of service as much as reasonably possible to prohibit various forms of harm at a more generic level than to invariably have to respond to the criminal laws of the various jurisdictions in which our users may be located.

18. We therefore commend an approach that would require OSPs to enhance or improve online safety by way of developing and applying robust terms of service.

7 – Should regulatory obligations depend on a service provider's risk or reach?

19. All OSPs are different, and the risk of online harm can vary significantly depending on a service's reach, the nature of the service, its user base, etc. MEGA therefore supports regulatory obligations being flexible in order to appropriately match OSPs.

20. That said, we are finding in the context of the UK Online Safety Act that defining a service's risk profile for the purposes of determining regulatory obligations is not straightforward. Reasonable minds may differ as to how risk is defined and how risky any given OSP may be in terms of online safety.

21. Reach, on the other hand, is much more straightforward to measure: we would expect all OSPs to know at least roughly the numbers of users they have in any given jurisdiction. It is an important metric that would also allow Australia to focus on the services that are the most

accessed by Australians. It will often align with an OSP's internal capacity to manage compliance matters (services with less reach are logically likely to be services with less resources). Our suggestion therefore is that obligations should be tied to OSPs' reach in Australia.

Part 3 – Protecting those who have experienced or encountered online harms

16 – What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

22. We note the processes in the Online Safety Act for the Commissioner to serve removal notices on OSPs, if alerted to unlawful content by a member of the public, as set out in the Issues Paper. While this may be a desirable process in some circumstances, we would observe that members of the public would obtain faster results if they simply come straight to us. We have a robust takedown process – where we are alerted to unlawful content being shared via our platform, we very promptly disable the relevant URL, terminate the relevant user's account, and in the case of child sexual abuse material or violent extremism provide details to the New Zealand Department of Internal Affairs. We anticipate that this is significantly faster than a removal notice process via a regulator.

23. Accordingly, we would suggest that an important part of educating the Australian public would be to make them aware of how they can contact OSPs directly to assist them in circumstances where they have encountered harmful content, in addition to approaching the eSafety Commissioner.

Part 5 – International approaches to address online harms

21 – Should the Act incorporate any of the international approaches identified above? If so, what should this look like?

24. As a general principle, we strongly support there being consistency between jurisdictions in terms of obligations imposed on OSPs. 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.

25. From our perspective, knowing that compliance with one online safety regime (say, the EU Digital Services Act) would also result in compliance with the Australian regime, would significantly streamline our efforts. It would be preferable if international regulators were able to acknowledge the standards imposed by other jurisdictions, and accept OSPs meeting requirements imposed by another jurisdiction as also being sufficient for their own jurisdiction.

26. Failing that, incorporating some of the approaches of other jurisdictions into Australian legislation or regulations may be preferable.

22 – Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?

27. MEGA has no difficulty with expectations, at a high level, that it aims to ensure its service can be used safely. Indeed, this is how we already operate. We also aim to incorporate safety by design. Where issues may arise is if the Act or any regulations try to specify what steps would be required to meet such expectations: this will vary significantly from OSP to OSP, depending on their user base, the nature of their services, and available resourcing.

28. Also difficult is the fact that compliance with a duty of care by an OSP is not easily measured. Nor can OSPs ever be solely responsible for online safety: bad actors will always exist to exploit online services and anyone using the Internet needs to be vigilant to protect themselves. It has long been the position that OSPs are not, generally speaking, liable for the actions of their users, and this is both a principled and practical approach – Mega, for example, is unable to monitor the content stored or shared by users unless it is reported to us so we ought not to be liable for its existence on our platform or its impact on other users when we are wholly unaware of it (and have taken all reasonable steps to inform users that such conduct is prohibited). These nuances create significant uncertainty and difficulty should Australia seek to impose an extended regime of penalties for non-compliance or create rights of claim for end users.

23 – Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?

29. MEGA is a long-time supporter of OSP transparency. We have been a member of the Tech Coalition's Transparency Working Group for a number of years, and we have been publishing our own transparency reports on a regular basis since 2015 (initially annually, but every six months since March 2022). As noted above, all current and historic data and reports are available at https://mega.io/transparency.

30. Currently, in the context of implementing the Digital Services Act, the European Union is considering imposing detailed requirements as to transparency reporting by OSPs. In particular, it appears that the EU will soon require transparency reporting to be undertaken in a prescribed format. Ofcom in the United Kingdom is also, we understand, considering requirements for transparency reporting.

31. MEGA understands the benefit of having consistent formats for transparency reports, to facilitate comparisons between platforms, and over time. However, each platform has different styles and volumes of usage and of misuse. Standardising a format to allow for all possibilities leads to a complex format that is daunting for smaller platforms such as MEGA. More daunting still is the prospect that differing formats may be required in different jurisdictions.

32. If the view is taken in Australia, therefore, that improvements are needed in relation to OSP transparency, we strongly urge you to ensure consistency with the requirements of other jurisdictions.

Part 6 – Regulating the online environment, technology and environmental changes

28 – What considerations are important in balancing innovation, privacy, security, and safety?

33. As we have explained, privacy and security are core values going to the heart of everything we do. As is stated in the Issues Paper,[3] E2EE is an "important defence against security breaches".

34. In August 2022, the United Nations High Commissioner for Human Rights affirmed the key role of encryption for privacy and security and human rights, outlining the various ways it helps protect people:[4]

> Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. Encryption ensures that people can share

[3] Page 52

[4] Report of the UN High Commissioner for Human Rights, 51st Sess., UN Doc A/HRC/51/17: The right to privacy in the digital age at 21. Available at https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age.

information freely, without fear that their information may become known to others, be they State authorities or cybercriminals.

35. Earlier this year, the European Court of Human Rights rejected a Russian law requiring "internet communication organisers" to, among other things, keep all messages sent by users for six months, along with a means to decrypt them.[5]

36. It is our view that an OSP using E2EE can be a responsible corporate citizen, enhance online safety, and provide a valuable contribution to the community at large. E2EE is not a barrier to efficiently and promptly taking action as soon as illegal content is reported as being shared on its platform.

37. In our most recent transparency report for the six months to 30 September 2023, Mega disclosed the very large number of accounts that it terminated for sharing objectionable material and also of links reported to contain child sexual abuse material that it terminated in the third quarter (Q3) of 2023. In Q3 2023, Mega processed over 1,200 requests for basic subscriber information from law enforcement agencies with a median response time of about 20 minutes. When we disable a link reported to us as sharing illegal material, we provide the details to the New Zealand Department of Internal Affairs (broadly comparable to American companies reporting to NCMEC). This demonstrates that E2EE need not be a hindrance to proper reporting or co-operation with authorities.

38. As a provider of E2EE services, Mega balances the above considerations every day by protecting the privacy, security and safety of our legitimate users and doing our best to combat unlawful or harmful content being stored or shared by non-compliant users.

39. Mega shares eSafety's view as expressed in its Updated Position Statement on E2EE in October 2023[6] that "safety, privacy, [innovation] and security are not mutually exclusive and each can be maintained through thoughtful and intentional design".

40. Ultimately, Mega's number one consideration when designing and developing our products and business practices is user control. This means implementing best privacy and security practices in the form of Safety and Privacy by Design. E2EE helps users protect themselves. By giving users control over their data and online interaction – i.e. by being user-centric and empowering them (each a fundamental principle of Privacy by Design and Safety by Design, respectively) and by implementing the most private settings by default in our products – our users are better able to restrict access to their data and online interactions to people they already know and trust.

41. E2EE also protects users, including children, from bad actors harvesting their personal data or intercepting and invading their communications. It also protects children from being 'datafied' (i.e. data minimisation prevents their personal data from being used for profiling and advertising) - a concern expressed in the Issues Statement.[7]

29 – Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?

[5] Podchasov v. Russia – decision available at https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}.
[6] Page 3
[7] Page 39

42. Mega's view is that the Act should remain technology neutral by applying a "reasonableness"[8] or "technical feasibility"[9] standard to the safety measures online service providers are expected to take under the Online Safety Act or under industry-specific codes.

43. A technology-specific approach is bound to become obsolete as technologies continue to evolve.

44. The introduction of a statutory duty of care or Safety by Design obligations would not change our response. For example, the duties imposed on online service providers in the UK Online Safety Act are duties to "take or use proportionate measures or systems"[10], and "to take appropriate steps".[11] What is proportionate or appropriate will vary from technology to technology, and from OSP to OSP.

45. Likewise, the principles of Safety by Design are well known[12] and how they should be specifically implemented by OSPs will also necessarily vary from technology to technology.

46. By way of example, Mega has found it challenging to engage with the UK Online Safety Act and in particular the extensive guidance prepared by Ofcom which attempts to regulate very particular aspects of a multitude of specific technologies. The UK Online Safety Act applies primarily to Mega as a provider of 'user-to-user' services (i.e. MEGA chat). However, much of the guidance is not pertinent to MEGA chat because our service was designed with safety and privacy in mind: users are in total control and empowered to accept or deny contact requests, join chat groups, etc. They are not put in a position where unwanted content can be served to them by anyone, be it other users or a recommender system (which Mega does not use). MEGA chat is not a specific technology that Ofcom appears to have contemplated would be covered by the UK Online Safety Act.

47. That said, if done well, a hybrid approach where the Online Safety Act remains technology neutral but guidelines or codes of conduct specific to certain categories of technology are issued can be an acceptable compromise. This assumes such guidelines or codes are prepared in consultation with the industry and remain non-binding so that OSPs retain the flexibility they need to implement more suitable measures to ensure their compliance with the Online Safety Act.

48. Ultimately, as set out above, Mega believes that regardless of the technology in question, putting the user in the centre and in control of their data and online interactions is the best way to protect innovation, as well as the privacy, security, and safety of legitimate users, thus preventing harm in the first place and enabling efficient and prompt action when harm is reported.

MEGA THE PRIVACY COMPANY

[8] As is done in parts of the Australian Online Safety Act
[9] As is done in parts of the UK Online Safety Act
[10] See Articles 10 and 12 https://www.legislation.gov.uk/ukpga/2023/50/enacted
[11] See Article 11 https://www.legislation.gov.uk/ukpga/2023/50/enacted
[12] 1. Service provider responsibility, 2. User empowerment and autonomy and 3. Transparency and accountability. See https://www.esafety.gov.au/industry/safety-by-design