INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

19 December 2023

Executive Manager
Industry Regulation and Legal Services
Office of the eSafety Commissioner

By email: submissions@esafety.gov.au

RE: Draft Relevant Electronic Services Standard and Designated Internet Services Standard

INTRODUCTION

The Internet Association of Australia (**IAA**) thanks the eSafety Commissioner for the opportunity to respond to the consultation being undertaken on the draft Relevant Electronic Services Standard (**RES Standard**) and Designated Internet Services Standard (**DIS Standard**) (together, the **Standards**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet Service Providers (**ISPs**). We understand that some of our membership may be covered by the Standards, namely the RES Standard due to the array of services provided by some ISPs, including telephony relevant electronic services and email services. To that end, this response is primarily in representation of these members. In addition, as an association concerned with and committed to the resilience and appropriate functioning of the Internet, our response also raises our concerns about the implications that the Standards may pose on basic principles associated with the Internet.

From the outset, IAA and our members recognise the importance of online safety, particularly in today's digital age where much of our daily life occurs online, including amongst children, and are therefore committed to taking action to ensure the Internet is a safe environment. We note the increasing concern for the proliferation of child sexual abuse material (**CSAM**) and pro-terror material (together, **harmful material**) online, and believe that an effective legislative framework is to the benefit of all stakeholders to ensure the growth and resilience of the Internet.

However, we are also committed to adhering to principles of security and privacy as well as the creation of measured and effective Internet policy. To that end, we are concerned that the Standards do not appropriately reflect a balance of these considerations. Overall, the Standards do not sufficiently reflect respect for the privacy of all individuals who would be affected by the requirements, and would also pose an unreasonable burden on industry. Furthermore, the Standards seem to encourage a culture of industry policing where the dissemination of harmful material should rather be dealt with by law enforcement in accordance with appropriate and clearly set out legislation.

OUR RESPONSE

Do the obligations on each relevant electronic service and designated internet service category appropriately reflect the above considerations? Are other considerations relevant?

We do not consider the obligations to reflect an appropriate balance of the considerations set out in the Discussion Paper, nor are the listed considerations sufficient to ensure a measured approach in balancing the safety of individuals, while also respecting the broader rights of privacy and burdens on industry.

Firstly, we believe that costs for industry to comply with the obligations and whether the benefit that would be achieved by each particular compliance measure would outweigh the costs, is an important factor that should be taken into account.

Proportionality should also be included as a consideration as it also relates to the characteristics of a service, and therefore the measures that different providers should implement in a manner that is appropriate to their business and services. We support the approach taken with respect to the development program requirement which is only an obligation for larger providers, and recommend that this approach be taken for other measures such as the annual compliance report requirement and the requirement to have personnel with requisite skills, experience and qualifications to ensure the provider' compliance with the relevant Standard. Our concerns regarding the effect of the Standards on smaller providers will be further discussed below.

We are also concerned that the obligations such as the detection and removal obligation do not sufficiently respect individuals' rights to privacy. While we appreciate the clarification in the Discussion Paper that the obligations do not require entities to take action that would subvert encryption, we note that:

1. This intention not to weaken or threaten encryption is not expressly set out in the draft Standards; and
2. This does not seem to be extended to the look-up phase prior to material being encrypted for end-to-end encrypted services, and indeed the obligation to take steps to detect harmful materials suggests industry should engage in client-side scanning.

Interfering with encryption poses great risk to security and confidentiality of the technical systems, as well as the trust and confidence that end-users have in use of digital services. Furthermore, these considerations are not divorced from online safety, and indeed privacy, and security of systems are paramount to online safety.

In addition, the obligation to otherwise disrupt and deter by taking other actions, wherein the Discussion Paper (though not the Standards) proposes industry could block the registration of certain classes of end-users who have distributed harmful materials from use of their services, not only increases the regulatory burden on end-users, but also raises other concerns about the balance between protection against harmful material, and the infringements to personal liberties. To outright restrict classes of people from utilising basic services raises broader legal and justice-related questions about the rights of the accused, or rights of criminals. To the extent that individuals are found using services inappropriately, including to disseminate harmful materials via the services, their access should no doubt be restricted. Indeed, this is already dealt with in section 14 of the respective Standards.

However, we believe it is inappropriate to give entities the power or responsibility to completely restrict certain individuals' use of services as common as gaming and email from the outset without proper procedures and in accordance with legislation, prior to such individuals being found or reasonably suspected to have been distributing or otherwise used in to access or solicit harmful materials. In particular, given that this suggested activity is only provided for in the Discussion Paper, rather than being clearly set out as a specific requirement in the Standard, this would gravely undermine the principle of procedural fairness. For the avoidance of doubt, we do not suggest that this is now further expanded upon to become a standalone obligation.

Nonetheless, if this is genuinely a necessary action that needs to be taken by service providers, it seems to be an area that requires greater consideration by legislators, in collaboration with the eSafety Commissioner and other stakeholders, to appropriately determine the proper processes that should be followed in outright banning individuals from utilising certain services. For example, there should be clearer limits set out such as repeated use of a similar type of service for the purpose of disseminating harmful materials. However, this clearly requires further consideration to ensure appropriate balance is being given to the rights of criminals as it points to further legal and philosophical issues and would have much more implications beyond in relation to online safety. To that end, it is not appropriate to deal with the matter simply by the Standards.

Is the test in section 5 workable? Is further guidance required to assist providers to determine whether this standard, or another code or standard, applies to a particular online service?

We believe that the application of the RES Standard is too broad, especially considering the existence of the recently registered online safety related ISP Code, as well as Part 15 of the Telecommunications Act (**Industry Assistance Framework**) and the Telecommunications (Interception and Access) Act 1979 (**TIA Act**). In particular, the Industry Assistance Framework applies to a broad set of communications, beyond that of traditional telecommunications, over which law enforcement and intelligence agencies can issue requests and notices for interception of communications. We believe this Industry Assistance Framework, alongside other measures including the TIA Act and other Online Safety related Codes sufficiently cover the telephony and email services (and other services) that fall under the RES Standard to ensure there are actions that can be taken in relation to harmful material being disseminated or stored on or accessed via such services.

Is the technical feasibility exception in the obligation to detect and remove known child sexual abuse material and pro-terror material appropriate? How effective will this obligation be with this exception?

We do not believe the standard for 'technical feasibility' provided in section 7 of the respective Standards are sufficient or appropriate in comprehensively addressing the nuanced balance that is required in the circumstances. Firstly, while clarified in the Discussion Paper, the Standards themselves do not explicitly set out that industry is not expected to take any action that would jeopardise or be otherwise counterposed to the resilience, security and strength of any encryption systems, and that this security consideration is a factor of technical feasibility. We recommend that this should be clearly set out in the Standards to ensure industry does not undertake any action that would so weaken encryption systems. Furthermore, the Standards should express that no action that would otherwise weaken the security of the service provider's system should be

taken. We also recommend that matters of privacy, and in particular, the reasonable cost/benefit analysis between the risk to the online safety of end-users and their privacy is also included in the Standards under the definition of technical feasibility.

Are the end-user reporting requirements workable for the relevant service providers? Are there practical barriers to implementation?

We believe the requirement to ensure the complaint mechanism do not require complainants to report via a separate web page or email address to be impracticable and unnecessary. We recommend that this is amended so that service providers should ensure their complaint mechanisms and processes are easy to find.

Furthermore, the compliance reporting obligations set out in section 37 of the RES Standard seems to be unnecessarily prescriptive. We recommend that the compliance report should only be required upon the eSafety Commissioner's request.

In addition, we are concerned that the RES Standard allows for the eSafety Commissioner to determine the periods provided to entities to produce certain reports such as the risk assessment, technical feasibility compliance and outcomes of development programs report, without any limitations. We recommend that the Standard sets out a reasonable minimum period such as 30 days to produce such reports, unless a shorter period is reasonably necessary in the circumstances.

What are your views on the likely compliance costs and, in particular, the impact of compliance costs on potential new entrants?

We believe that these Standards would result in great cost for industry, particularly given the increasingly complex regulatory matrix that telecommunications providers find themselves in, regardless of how many will be specifically captured by these Standards. In particular, in light of our members, who represent the smaller entities in the industry, these Standards pose great operational costs, as well as costs related to unpacking, understanding and implementing regulation.

Indeed, the requirement to have suitably qualified and experienced personnel to ensure compliance with the Standard in section 18 and 20 of the RES Standard and DIS Standard respectively, is vague and could suggest a regulatory officer with legal or other such background is required within an organisation. This is not feasible for many smaller organisations who do not have the resources to staff such personnel. We note that this is not further clarified in the Discussion Paper nor the respective Fact Sheets to assure providers of the level of skill or nature of experience and/or qualifications required to fulfil this role.

Furthermore, the implications some of these compliance measures will have on an entity's other legislative obligations such as with respect to the *Privacy Act 1988* (Cth) will also need to be considered in greater detail. Thus, entities will have to deal with costs associated with navigating the complex and at times, conflicting web of regulation.

The imbalance in competition in the telecommunications market is already clearly evident, and imposing the great costs associated with the Standards will only exacerbate the issue. This is especially the case for those providers who provide other services such as email hosting on top of

standard telecommunications services as an additional offer to incentivise customers. This will also increase the barrier to market entry, further stifling competition. This is not in the interest of end-users as Australians have less choice in providers.

We reiterate the robust legislative framework that exists under the TIA Act and Industry Assistance Framework that allows for law enforcement to take appropriate action in response to sharing of communications that includes the harmful communications the centre of the Standards. To that end, we believe that the overall cost is not only to industry, but to all end-users, by imposing such great burdens on industry to comply with the Standards is not appropriately balanced.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Relevant Electronic Services Standard and Designated Internet Services Standard. As aforementioned, we are committed to ensuring online safety, and working with the eSafety Commissioner to that end. However, we are concerned that the Standards in their current form do not appropriately balance the myriad of considerations that must be had to ensure an online safety framework that is also cognisant of individuals' rights to privacy, other individual liberties, as well as the importance of the security and resilience of systems, costs to industry, and the broader impacts these considerations have on the overall safety of end-users online, which goes beyond protection from harmful material. We are thus committed to continue working with the eSafety Commissioner and other stakeholders to develop Standards that appropriately and effectively deal with the issue of online safety in a nuanced manner.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth. IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia