[redacted]

[redacted]

Dear Office of the eSafety Commissioner,

This submission is from [redacted] I may be identified as "A.M." in any publication referring to my submission. I may be contacted at [redacted] (note: email address is confidential and not for publication). Please find my submission inline below.

Kind regards,

[redacted]

I would like to begin my submission by commenting on the adequacy of your consultation process. I took all reasonable steps to learn about eSafety industry standards and codes coming into force; I submitted on the industry code consultations, I signed up for the "eSafety news" on your website, and I signed up to learn about government consultations at https://consult.industry.gov.au/. However, despite all these proactive steps, I first heard about both the industry codes coming into force, and about the consultation on this industry standard through the press a few days before submissions were due to close. This has forced me to make this submission with limited time, and it is fortunate that I heard about it at all. A consultation where even parties who take proactive steps to ensure they are informed of open consultations aren't informed is not a genuine public consultation, and I would encourage your office to at least inform people who have signed up to your newsletter of consultations.

As I shall explain, there is also a process deficiency in industry code process followed to date under section 141 of the Online Safety Act 2021, and this deficiency means that the existing codes purported to be registered under section 141 are not validly registered. In addition, as the purported consultation under section 141 was not valid, the trigger allowing the eSafety Commissioner to determine an industry standard has also not been met.

The specific deficiency is that there is a significant subset, specifically individual and non-profit providers of services and software, of each of the "section of the online industry", as defined in the Act, that is not validly represented by the bodies or associations selected by eSafety as the recipient of a request under section 141.

A significant proportion of Internet services are not operated by large corporations, but are instead operated by individuals and not-for-profits. In the early days of the public Internet, the majority of interaction was with smaller non-commercial services. More recently, a significant proportion of traffic is to large commercial players, but smaller players, including self-hosted services, still exist, and indeed likely dominate in terms of numbers of sites (even though they do not dominate in terms of traffic). With the emergence of concepts such as the fediverse, and better technology for self-hosting, services hosted by individuals and small non-profit organisations (whether incorporated or not) are making something of a resurgence.

However, all of the bodies involved in the development of the industry codes are only representative of large commercial players. All of them have some policy or practice or another that exclude hobbyists. Common means of exclusion include not allowing individual members such as hobbyists, charging fees that would be prohibitively expensive for a hobbyist, and requiring commercial activities. AMTA represents "mobile network operators and service providers, mobile phone and device manufacturers, retail outlets, network equipment suppliers and other suppliers to the industry" - all businesses - and does not have a single individual member listed on their membership

list. BSA membership is exclusively for companies. Comms Alliance technically has individual members, but firstly, they are not truly represented by the body (the constitution says, for example, that they have no vote at meetings), and secondly, Comms Alliance has only one individual member - the head of a law firm and not a hobbyist - who is not an honorary life member. The other individual members are all honorary life members who obtained the position through their work representing companies or as employees / officeholders of Comms Alliance. Digital Industry Group defines themselves as "the industry association for companies that invest in online safety, privacy, cyber security and a thriving Australian digital economy"; they only represent companies and have no individual / hobbyist members. The Interactive Games and Entertainment Association is primarily focused on representing business interests of members, and charges a $500 per annum fee (which is enough to discourage nearly all hobbyists, who by definition do not profit from their hobby). Full memberhip requires at least $1M in annual turnover, clearly disqualifying hobbyist members.

As such, none of the bodies consulted represent hobbyists / not-for-profits self-hosting services. However, individual hobbyists and not-for-profits do form part of the "section of the online industry", as defined in the Online Safety Act 2022; definitions are all along the lines of "the group consisting of providers of relevant electronic services, so far as those services are provided to end-users in Australia". Hobbyists are providing a service to members of the public who use the systems they build, and if that service meets the definition of "relevant electronic service" by virtue of its functionality, then that makes the hobbyist part of the section of the online industry, but one that was not represented in the section 141 request. I submit that the Online Safety Commissioner ought to have reasonably known of the existence of hobbyists given her role, and therefore the Commissioner should not have been satisfied that the bodies or associations truly represented the section of the online industry.

The impact of making the section 141 request without representation for non-commercial providers (hobbyists / not-for-profits) is not a mere technicality. Submissions made on the codes around impact to non-commercial providers were largely ignored by the bodies; in some cases the response in the summary from the consultation was that they didn't understand terminology common in the such as fediverse (despite this being common knowledge amongst hobbyist providers, and despite information being freely available on the Internet). There was a clear misalignment of incentives; commercial players actually benefit from squeezing out non-commercial players who would compete with them through regulatory capture and codes and standards that are onerous for individual providers. Non-commercial providers are motivated to provide a human-focused Internet the focuses on what is good for people, while providers with a profit motives instead seek to build large walled gardens powered by algorithms that optimise for engagement - even if rage driven - that are bad for the collective eSafety, and increase the risk profile. It is therefore in the public interest that the Act be followed, and a truly representative body be requested to provide the code. As such, the section 141 requests should be treated as having never been validly made. As a flow on consequence, the Industry Standard should not be purported to be made under section 145 unless this is first rectified.

On the specifics of the proposed industry standard, I make the following
points:

In section 6, in the definition of "gaming service with communications functionality", subsection (e): I suggest changing "any or all" to "one or more", to permit the possibility that more than one, but less than all of the material types are allowed. I suggest adding "(vii) Hyperlinked text that is subject to automated filtering technology, which only permits hyperlinks to a pre-approved list of services, and where the provider is satisfied that all services on the pre-approved list take reasonable measures to protect the safety of Australian users, and has a process to review the list following any complaints". This will provide an easy mechanism to allow hobbyist game developers to still allow hyperlinks (for example, to external chat systems such as Discord, or to specific wikis that comply with the Industry Standard).
If the destination service the link goes to itself has robust processes, then the risk to users is very minimal. This avoids the disproportionate outcome of classifying such a service as a pee-assessed relevant electronic service, and the significant burden that would impose on hobbyist developers (not to mention on the eSafety Commissioner in terms of processing a deluge of annual reports for games potentially with only a few users).

In section 6, definition of "pre-assessed relevant electronic service", I suggest appending, "and which has at least 1,000 active monthly end-users". The burden on operators of such services is otherwise disproportionate to the risk.

At subsections 19(9)(a), 28(3), and 32(2), there is text saying "that is, not on a separate webpage to the webpage for the service". This does not make sense for all services. Firstly, not all services are web based, and it is not clear how to comply in the event of a non web-based service. Secondly, if we suppose it is a web application, there are multiple technologies for implementing web applications. Some applications are built as 'single page applications' where navigating internally in the application (including by clicking on what look like
links) does not re-load the site, and merely brings up different screens. In applications work by navigating to different pages regularly as the application is used. This is generally considered an internal technical detail - it can be relatively transparent to a user. In some cases, providers migrating functionality might have two single-page applications and put old functionality on the old page, and new functionality on the new page. Given that which webpage content is on is an internal technical detail which has very limited bearing on the experience of how easy or difficult it is to navigate to material, and in some cases it could be burdensome to replicate the same content into a legacy single-page application, it seems like this is not an appropriate way to ensure material is easily accessible. It is not entirely clear what the goal is; it would be preferable to have the information available with one click on a different page, than with 10 clicks in a single page application. It would be better to simply say the material must be "easily accessible", and leave the implementation details of how to make it easily accessible up to the provider.

At section 15(4), there is a requirement to "as soon as practicable, notify an organisation that verifies material as pro-terror material".
However, it is not clear such a service exists. The top 30 or so results at least in Google for report "pro-terror material" are either about the activities of the eSafety Commissioner, or are policies apparently written to comply with the Australian code about reporting content to specific providers of services.

At section 18(3), requiring individual hobbyist providers of tiny pre-assessed relevant electronic services to have staff to supervise the service "at all times" is disproportionate - it is effectively saying that an individual providing a service for the benefit of the community needs to be on-call 24x7 without ever taking a break, which is likely to cause burnout, and would be a net negative for eSafety. Hobbyist providers are a valuable part of the online community, and this would be a net negative for society.

At section 19(7), these requirements essentially ban services without use registration. This is not the norm for many open protocols (such as Internet Relay Chat, which is a standard protocol that is the first ever chat protocol), and Jabber. Most of these services require selecting a username and password to register, or in some cases, upon connecting, provide a nickname; it is not clear if a username is a sufficient 'identity', as this term is not defined. In any case, this would break widely established and widely used protocols currently in place by smaller providers across the world (if actually implemented; in practice, if it is too onerous, it will be ignored by small overseas players, which is a worse outcome than making an achievable measure and trying to work with such providers). The classic abuse control mechanism on IRC and similar protocols is to ban users by IP address if they repeatedly break rules; this is generally adequate, and there is no real benefit to the friction of requiring any user-provided identifier (which, after all, users can easily obtain anonymously anyway).

At section 20(4), it is also not clear how an individual hobbyist would obtain any database of perceptual hashes to check images from a provider such as the NCMEC. There is not even a form to apply for access to the database - it seems to only be for big providers only. The definition seems to apply that if it is on any database anywhere, it needs to be detected, even if the provider has no access to the database. It should be limited to data which has been provided to the provider - the onus would then be on database maintainers to reach out to providers if they wish for that provider to filter their content. A similar concern applies to section 21.