Mark Nottingham
[redacted]

Submission to the Statutory Review of the Online Safety Act 2021

21 June 2024

Minister Rowland and Ms. Rickard,

Thank you for the opportunity to make a submission.

To introduce myself briefly: I have contributed to Internet and Web standards and governance for approximately twenty five years. Formerly, I have been a member of the Internet Architecture Board and a member of the W3C Technical Architecture Group. Currently, I chair the IETF HTTP Working Group and am a member of the Board of Directors of the World Wide Web Consortium. While my submission is informed by my experience in those positions, I write it solely as an individual.

I am supportive of efforts to improve online safety, and believe that the eSafety Commissioner's actions and activities contribute meaningfully to it. In particular, her focus on holding 'big tech' companies to account regarding the safety of Australian Internet users is admirable.

However, I am concerned that the Online Safety Act grants the Commissioner much broader powers than are intended, and that there are insufficient checks on them. Furthermore, she is not required by the legislation to balance the goal of online safety with other, equally important societal goals, and has failed to do so in the recent past.

Three examples can illustrate the impact of this combination.

First, the Act empowers the Commissioner to accept Industry Codes and to impose Industry Standards. As drafted, however, the legislation applies to much more than just 'industry' -- it effectively applies to all Internet communication, no matter what the source.

While Facebook, Google, Twitter (now 'x.com') and similar companies are a large part of Australians' Internet experiences, both our use of the Internet and its promise are much more than these 'big tech' companies. Australians can and do host their own Internet services -- everyone from local footy clubs, community groups, churches, non-profits, and individual hobbyists to families.

However, because of how the Act is written, almost any Web server or similar software is captured -- even if it only available to a single person on their own computer.

As a result, there is the potential for significant regulatory burden on these services, with requirements to hire 'a person with the relevant skills' to perform a risk assessment.[1] Besides their intrusion on freedom of association, it is likely that such requirements will have the effect of discouraging development of small, new competitors to 'big tech' platforms, leading to impact on both trade and competition.

Colleagues and I have brought these concerns to the attention of the Commissioner,[2] but there has not been any substantial response to them.

Second, the Commissioner has regularly and repeatedly pressured industry to insert so-called 'client-side scanning' into encrypted applications.[3]

Putting aside the grave risks that that Australians would be exposed to by such requirements, it is dangerous and inappropriate for such important questions of policy -- with serious implications for security, industry, human rights, and trade to be driven by a Commissioner who is only charged with assuring online safety.

Contrast Australia's approach to that taken in Europe,[4] where European Parliament considered the matter directly. This is a question for democratic societies to address using all of the mechanisms at their disposal to assure a legitimate and accountable solution, not something for Parliament to delegate to an accountable, opaque decision by one person.

Third, the Commissioner has recently attempted to apply Australian standards to content both viewed and hosted overseas.[5] Again, this is an important matter that

[1] See <https://www.mnot.net/blog/2023/11/27/esafety-industry-standards>.

[2] See eg <https://www.mnot.net/papers/22-09-esafety-industry-codes.pdf>.

[3] See eg <https://www.esafety.gov.au/sites/default/files/2023-10/End-to-end-encryption-position-statement-oct2023.pdf>.

[4] See <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN&qid=1652451192472>.

[5] eSafety Commissioner v X Corp [2024] FCA 499.

involves far-reaching issues such as Internet governance, impact on human rights overseas, and foreign relations.

That is because the Commissioner's actions can be used to justify similar actions by less well-intentioned regimes: for example, other countries might use it to justify their own orders to remove political content worldwide. As such, her actions can be seen to contribute significantly to the fragmentation of the Internet, and is a significant example of a failure to balance safety of Australian Internet users with other important considerations.

With these examples in mind, I turn to selected questions in the Issues Paper.

Responses to the Issue Paper's Questions

3. Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?

Yes. As discussed in the first example above, the Act does not just regulate 'industry,' it regulates all communication on the Internet in Australia, no matter what its nature.

Of particular concern is the regulatory burden imposed upon individuals and non-profit entities, and the resulting tendency to reinforce the hold of 'big tech' on Australians' use of the Internet. Uncertainty about the effects of regulation can have similar effects as well.

For example, the 'Fediverse'[6] is emerging as a community-led, decentralised alternative to centralised and advertising-supported services like x.com, Threads, Instagram and Facebook. This phenomenon shows great promise as a means to promote Australia's digital sovereignty, make markets like social media more contestable and competitive, and put control of their digital lives back into Australians' hands.

However, volunteer-led, community Fediverse services like Mastodon fall under the same regulatory regime as these well-resourced companies in Australia. They are not equipped to handle the regulatory burden, and the associated risks, penalties, and doubts will dissuade many services from being established.

[6] See eg, <https://www.theverge.com/24063290/fediverse-explained-activitypub-social-media-open-protocol>.

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 code drafting process be improved?

Because the Internet is much more than just 'industry,' having policy proposals only made by limited-participation industry associations is completely inappropriate, and creates a risk of industry using the codes as a mechanism to discourage competition from newcomers or Australians who wish to use the Internet without 'big tech'.

See below for suggestions regarding legitimacy of process.

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

Yes. Per above, the obligations need to be proportionate to the reach and nature of the service provider. While the Commissioner has proposed measures to graduate obligations, they do not accommodate the full range of services available and present on the Internet today in Australia.

In particular, there is little benefit to requiring very small, non-commercial services to perform risk assessments. The eSafety Commissioner already has powers that allow her to address any such problematic content held by these services, and a risk assessment done as 'compliance theatre' is unlikely to significantly make the Australian Internet safer.

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

No. From speaking with colleagues in the technical community and civil society, the eSafety Commissioner seems to have developed a reputation of being opaque and selective in consultation. Likewise, there are many stakeholders who are denied access to the industry codes process.

If the Act retains its current scope, a much more inclusive, transparent, and accountable process is necessary to assure that all relevant concerns are represented and balanced. This likely would involve removing final decision making authority from the eSafety Commissioner on items such as the acceptance of codes and standards.

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

Myriad considerations are important, but most of all the entity performing the balancing needs to account for them all and be accountable to the Australian people. The Act currently does not address this balance, much less promote it.

32. Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?

No. Because of the mismatch in scope and powers explored above, the Online Safety Act fails to create an accountable, legitimate governance regime.

Internet governance is complex, messy, and dynamic. While it is understandably attractive to subsume all other concerns to safety and delegate authority to a third party, it is not the act of a responsible, democratic government to do so.