With respect to the Frequently asked questions: the suggested “reasonable steps “ for encrypted services appear to be steps already obligated under metadata retention, with obligations placed further on service owners over law enforcement.

> *Providers of encrypted services are expected to proactively address and mitigate unlawful and harmful activity on their services. Reasonable steps might include a range of actions, such as detecting misuse through behavioural, account or online signals including routing information and metadata and closing accounts.*

With respect to the Determination itself:
6 (2) - “...proactively minimise the extent to which material or activity on the service is or may be unlawful or harmful.”

- I note the Act itself does not define “harm”
- The lack of any definition of harm in this determination, then, begs the questions “harmful to whom”, “harmful in what regard”, and “harmful by whose standard?”
- There appears to be a real danger of this determination being weaponised on purely religious and/or subjective morality grounds in order to silence or interfere with communication.
- As a principle, should we not also be concerned about ensuring that open exchange of ideas is preserved, and that content one *simply disagrees with* is not subject to definition of “harm”?
- The question of “harmful by whose standard” is important. I could contrast the harms of spreading medical mis/disinformation via social media as harmful in a scientific evidence standard, with the harms caused in illegal sharing of child exploitation material and the legal standard that applies, with the very largely subjective moral concerns related to sharing adult material between consenting adults and the apparently moral standard that applies.
- Without addressing these questions, the very “broadness” that this determination has tried to preserve risks being used to stifle and silence, and to ensure that service owners have no choice but to treat spurious complaints as genuine.

7 (1) and (2) - “...service will consult with the Commissioner”, contrasting with “...have regard to any relevant material made available by the Commissioner”

- “Consult with” and “having regard for published material” are not consistent. Reading fact sheets is not consultation.

8 - “If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful.”

- I note that there are no example reasonable steps published in the draft determination, only examples published in the “frequently asked questions”.
- If we read this as a statement of principle, further principles around implementation should be considered.
- For example
    - Is it “reasonable” to undermine the encryption itself? Under what circumstances, if so? (This could include - service operating as a ‘man in the middle’ on encrypted comms, thereby seeing all interchanges unencrypted)
    - Is it “reasonable” to alter the fundamental design of the service to better support this principle? To what extent, if so? (This could include - alterations

to the service itself such that users can be uniquely identified, alterations to the service itself such that users interact via an Identified pathway, such as mobile phone)
    - Is it “reasonable” to reduce the quality of the service to prevent even the possibility of certain media being exchanged?
- Please note, importantly, that the principles that underpin this “reasonable steps” intention must further be consulted. I would contend that this point can not be meaningfully assessed without this additional information.

10 (2)(b) - “sharing information with other service providers on material or activity on the service that is or may be unlawful or harmful...”

- Please see my earlier remarks about how “harmful” should be interpreted in this determination.

12 (2) - “reasonable steps for the purposes of that subsection could include the following” (a) “implementing age assurance mechanisms”

- This statement is especially worrying. The suggestion that age assurance mechanisms being implemented should be considered as “reasonable” without limitation needs to be considered in light of the harms associated with the gathering of that data in the first place and the potential harms for inevitable failures to protect that data.
- If we are truly concerned for the safety of children, it appears to me that services having *less data* instead of more does more to preserve that safety than any other step we might take.
- At a minimum, consider that it may be possible to assure age without ever storing or sighting personal information, and explicitly stating that increasing the privacy risks to children is not the intent of the Act nor the Determination.
- While nothing has been said to this effect, it may also be useful to include “what is *not* reasonable?” (Suggested inclusions: any machine learning / AI approach to interpreting photos, any facial recognition, upload and storing of birth certificate, a child directly interacting with employee of the service in order to demonstrate age)