

To whom it may concern.

The industry standards recently proposed by the eSafety Commissioner are reasonable in concept, however the incorporation of techniques such as client-side scanning is invasive and potentially unsafe.

Any backdoor into encrypted data can and will be accessed by criminals. I and many others urge you not to mandate such practices. While I understand the issue with child sexual abuse material, terrorism, and other forms of illegal content, mandating that providers of encrypted services incorporate a method in which encrypted, illegal content can be flagged and/or removed (such as back doors or client-side scanning) will allow hackers to abuse the methods implemented, putting millions of innocent Australian civilians, businesses, and anyone who communicates with them at higher risk of blackmail and identity theft.

In conclusion, while the flagging and removal of illegal content is an important matter, the methods proposed will cause more harm than good for the Australian people and potentially the world. Having publicly stated that the eSafety Commissioner has no intent to undermine end-to-end encrypted services, it it disappointing to see these invasive standards being proposed. I urge you to search for other methods of detecting illegal content that do not jeopardize the privacy and security of innocent individuals.

Thank you for reading,

Twish for my name and contact information to remain confidential. For publication purposes, please refer to me only as "Anonymous"