FEEDBACK ON AN EXPOSURE DRAFT ONLINE SAFETY BILL FROM

CHARLES GUTJAHR

14 February 2021

I am providing feedback on the exposure draft Online Safety Bill based on my industry experience. I have worked as a programmer and systems architect for online services for 20 years. The services I have worked on are not social media and likely not directly subject to the Bill, but I believe my experience has provided me with relevant insight to how the Bill may affect such services. The opinions in this submission are my personal opinion and not that of my associated businesses.

In general I support the objects of the Act to improve and promote online safety for Australians. I think that it achieves that in some areas and fails in others. I have two concerns in particular:

- A restricted access system may aid criminals
- Industry codes may overcensor and restrict normal speech

A restricted access system may aid criminals

Section 108 declares that the Commissioner may declare that a specified access-control system is a restricted access system. The section identifies areas the Commissioner must have regard to but does not list security or privacy. I am concerned that could result in the Commissioner declaring access control systems which are insecure and so aid criminal activity.

The purpose of an access-control system is to confirm that the person is an adult, and so it is very likely that such a system would ask for personal information to verify age. Such a system may require a person to provide sensitive documents such as a drivers license or passport by uploading photos of the documents to online services.

This makes an access-control system a high value target for criminals. A criminal who can successfully hack into such a system would have access to some of the most detailed personal information available for identify theft. They could use this to commit crimes under a false identity, create fraudulent loans, launder money, and many more crimes.

This would especially be a risk during the transition period of the bill. In my experience it can take several years to develop an online system which handles personal information with a high level of security and privacy controls; a minimum viable product can be implemented in a few weeks but such a product will contain bugs (mistakes) and be relatively insecure. If there is a rush from industry to implement access-control systems to meet a short deadline for the introduction of the bill then I expect those systems have insufficient security and be at high risk of hacking and criminal activity.

At a minimum section 108 should direct the Commissioner to regard security and privacy in declarations.

However even better would be for section 108 to specifically disallow access-control systems to require sensitive documents such as drivers licenses and passports. Even the most robust online systems are at risk from hackers. Large international companies such as Adobe, Sony, and Vodafone have been successfully hacked for personal information despite the large investment they make in security. It is reasonable to assume that an access-control system which stores personal information, drivers licenses, and passports *will* be hacked by criminals because it is such a high-value target. The only way to ensure criminals cannot do that it is to not make such personal information available online.

It is worth considering whether the Bill should address access-control systems at all. In my opinion access-control systems would do little to achieve the stated aim of the Bill because they would not prevent children from accessing restricted content from overseas services. Yet they bring a significant risk of criminal activity. In my opinion access-control systems will do more harm than good, and so should not be legislated or required in Australia.

Industry codes may overcensor and restrict normal speech

The Bill encourages industry to develop and apply industry codes related to online safety. I am concerned that these will result in overly strict interpretations to avoid any liability under the law. In other words: removing content at the slightest hint of a problem to avoid liability, instead of assessing whether the content should reasonably be published. The result would be normal speech being restricted unnecessarily, with decisions made by an unaccountable private company which may not be based in Australia.

I can give a specific example of an experience I had with Facebook in 2019. Though the content in my example would not be covered by this Bill the same scenario would apply to such content.

In February 2019 a friend of mine posted an image on Facebook of his new business logo. In response I posted a comment warning him of some accidental similarities to Nazi imagery in the logo. He appreciated the feedback; there were no concerns from him about my comment. However soon afterwards Facebook deleted my comment and gave me a formal warning that I had violated their Community Standards. They gave me no recourse: there was no facility to argue that they were mistaken; as far as I know I had not violated the standards or any law but their judgement was final and unquestionable, and my comment deleted.

I expect this overzealous deleting of content will also occur in an industry code encouraged by this Bill. Facebook has already been embroiled in controversies about content being falsely interpreted as sexual which should not have been; take for example breastfeeding photos, or the famous photo of Phan Thi Kim Phuc taken during the Vietnam War. Outsourcing the policing of community standards via an industry code risks important social and historical information being banned by private foreign companies who are not answerable to the Australian people.

Sincerely,

Charles Gutjahr