Draft Online Safety (Basic Online Safety Expectations) Determination – Submission to the Department of Infrastructure, Transport, Regional Development and Communications

To the Department of Infrastructure, Transport, Regional Development and Communications, I'd like to thank you for the opportunity to provide a submission for the consultation into the draft Online Safety (Basic Online Safety Expectations) Determination.

I believe that online safety is an important issue to address in Australia, and globally, however I have several concerns about the Online Safety (Basic Online Safety Expectations) Determination which I have outlined below for your consideration:

Concern 1: Provider Will Take Reasonable Steps to Ensure Safe Use

My concern with this expectation is that because the principals are quite vague and the Expectation are intended to read in the broadest sense are open to interpretation by service providers, without better defining what "unlawful" or "harmful" is, the Expectation provides too much latitude for service providers.

If "unlawful" or "harmful" are not defined as outlined in Expectation 11, this must be made clear – else service providers may start to proactively remove media based on moral standards felt by content moderators, provider employees, or their board members.

The recommendations made by in the Global Partners Digital & Digital Rights Watch submission regarding artificial intelligence controls should be strongly considered by the committee.

Concern 2: Provider Will Take Reasonable Steps Regarding Encrypted Services

My concern with this additional expectation is that there seems to be disagreement between the FAQ document and the outcome sought by the determination. In the FAQ document, encryption is framed as the enemy of online safety, giving the example that encrypted communication "can be used to share material or conduct activity that is unlawful/or harmful" however, we know the encryption also provides nearly every single Australian:

- Encryption protects the privacy of its users – from example tax return documents, banking forms and other forms of sensitive data.
- Encryption prevents identity theft and blackmail, and
- Encryption allows the transmission and sharing of sensitive forms and files.

Furthermore, encryption is used by service providers to ensure personal and private health data isn't misused, lost or accessed by employees who are not permitted to access that information and acts as a form of harm reduction in online spaces.

This expectation as it's currently worded should be removed from the determination and replaced with an alternative that stipulates that regardless of the encryption usage the provider will take reasonable steps to detect and address material or activity on the service that may be unlawful or harmful.

This is especially important considering the FAQ outlines providers could meet this expectation via behavioural, account or online signals.

Concern 3: Provider Will Take Reasonable Steps Regarding Anonymous Accounts

Most websites require users to already verify their account by confirming ownership of an email address or mobile number, while other services require users to provide identifying information or documents like passports, drivers licenses or other documents depending on the number of points needed.

The trouble is many of the services that require more aggressive forms of identification do not consider the implications of how that may impact marginalised groups who don't or can't get access to various forms of identification. Furthermore, there is often no consideration for people who due to family violence have their identity documents controlled as part of coercive control.

Therefore, it is my belief that this additional expectation and associated reasonable steps should be removed from the Act. Instead, the Committee should consider instead adding in an Expectation that allows users to select who they can and cannot interact with, for example: Block Party App founded by Tracy Chou provides powerful functionality to set filters on Block Party to determine who you want to hear from in your Twitter mentions – this sort of system has allowed people from a variety of background to take back control of how they interact with people within their social networks.

Thank you for your time in reading over my concerns and recommendations regarding the Draft Online Safety (Basic Online Safety Expectations) Determination.