

15 March 2023

Legislation & Policy Branch
Office of the Commissioner
NSW Police Force

Via email: legpol@police.nsw.gov.au

Re: Consultation on proposals to amend the Child Protection (Offender Registration) Act 2000

The eSafety Commissioner (eSafety) welcomes the opportunity to provide a submission to the NSW Police Force's consultation on proposals to amend the *Child Protection (Offender Registration) Act 2000* (the Act).

As Australia's regulator for online safety, eSafety's core objective is to minimise harm to Australians online. We commend and share the Act's purpose to protect children from serious harm and ensure the prevention and early detection of offences by repeat child sex offenders.

eSafety's role addressing child sexual exploitation material

When eSafety was formed in mid-2015, part of our remit included administering the Online Content Scheme. This empowered eSafety to investigate complaints and facilitate the removal of prohibited content hosted in Australia, including child sexual exploitation material (CSEM).

In January 2022, the *Online Safety Act 2021* (Cth) (OSA) came into effect and introduced new powers for eSafety, including strengthening and extending our existing powers under the Online Content Scheme.

The OSA also provided eSafety with new tools to regulate services' systems and processes, including the power to require online service providers to report on the steps they are taking to comply with the Basic Online Safety Expectations, which outline the Australian government's expectations for certain types of online services to minimise material or activity that is unlawful or harmful. In addition, the OSA provides for the online industry to develop new industry codes to combat illegal and restricted content, including CSEM.

eSafety actively works with relevant state, territory, and federal law enforcement agencies to combat CSEM and offender activity online. This includes the NSW Police and the Australian Federal Police (AFP)-led Australian Centre to Counter Child Exploitation (ACCCE).

In February 2023, eSafety expanded its Memorandum of Understand (MoU) with NSW Police, which formalised updated protocols for cooperation when addressing the availability of child abuse material online.

Personal information required to be reported

eSafety supports Proposal 5.5, which would require additional information, including social networking platforms or apps used as well as websites owned and managed, to be reported as 'personal information' of repeat child sex offenders.

Having repeat child sex offenders report these online accounts can have several benefits, such as enhancing identification and monitoring capabilities for law enforcement, deterring recidivism through stronger legal consequences for child sex offenders, and contributing to greater public safety.

Our research and investigations show that multiple types of online services continue to be used to groom and abuse children and young people, and access and share child sexual exploitation material. For example, an offender may use social media, dating, or gaming services to ‘discover’ children, before moving them to more direct contact on messaging and livestreaming services. Offenders can then store and/or share abuse content using cloud storage and files sharing sites, as well as messaging services, particularly those which are end-to-end encrypted.

Any interventions must look across the whole online ecosystem. We suggest that reporting requirements under the Act are flexible enough to capture broader types of online services, including new and emerging services such as immersive technologies. This would also align with the OSA, which applies to a range of online services, such as social media services, electronic services, and designated internet services.

We also note that registration of social networking platforms for child sex offenders is already legislated in other Australian states and territories. For example, Section 10A of the Queensland *Child Protection (Offender Reporting and Offender Prohibition Order) Act 2004* requires offenders to detail either their email address, username, or identity associated with an instant messaging service, including any changes. It also requires details of reportable offenders’ telecommunication carriage services and internet carriage services used.

Over 2022-23, the Queensland Parliament’s Community Support and Services Committee consulted on amendments to the Act, including whether greater restrictions were needed to reflect advances in anonymising and encryption technologies. eSafety contributed to these discussions and would encourage coordinated responses across Australian state and territories.

eSafety looks forward to continued work with NSW law enforcement to address our common goal of protecting children and young people.

Yours faithfully,



Toby Dagg

A/eSafety Commissioner