Australian Government | eSafetyCommissioner

eSafety Submission

Consultation on the Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022

November 2022

Foreword

The eSafety Commissioner (eSafety) welcomes the opportunity to provide a submission to the Queensland Parliament's Community Support and Services Committee's consultation on the Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022 (the Bill).

As Australia's regulator for online safety, our core objective is to minimise harm to Australians online. We commend and share the Bill's objectives of safeguarding the online experiences of children and protecting their sexual safety. eSafety agrees that our nation's legislation should anticipate and respond to advancing technologies that enable offenders to harm children and evade detection. Reducing the likelihood and opportunities for offenders to re-offend is an important part of broader efforts to prevent, detect and hold perpetrators accountable for child sexual abuse and exploitation.

This submission draws on our role and experience in addressing child sexual exploitation material (CSEM) online, as well as our observations of existing and emerging technologies, including anonymising and identity shielding tools and end-to-end encrypted (E2EE) services.

About eSafety and our role addressing CSEM

eSafety is the first regulator in the world dedicated specifically to online safety. We lead, coordinate, educate and advise on online safety issues and aim to empower all Australians to have safer, more positive online experiences.

When eSafety was formed in July 2015 (as the Children's eSafety Commissioner), part of our remit included administering the Online Content Scheme. This empowered eSafety to investigate complaints and facilitate removal of prohibited content hosted in Australia, including CSEM.

Since then, eSafety's functions have broadened to further protect both children and adults online. 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 and our other schemes relating to image-based abuse and cyberbullying.

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. There are specific expectations regarding encrypted services and services that permit the use of anonymous accounts.

In addition, the Act provides for 8 sections of the online industry to develop new industry codes to combat illegal and restricted content, including CSEM. Upon registration, the industry codes would create obligations for providers of social media, messaging, search engine, app distribution services, as well as internet and hosting service providers, manufacturers and suppliers of equipment used to access online services and those that install and maintain the equipment.

eSafety actively works with local and global stakeholders across multiple sectors, including relevant law enforcement agencies, to combat CSEM and offender activity online. This includes the Queensland Police Service's Task Force Argos and the Australian Federal Police (AFP)-led Australian Centre to Counter Child Exploitation (ACCCE), the national coordination mechanism for online child sexual exploitation and abuse.

Further details about our role, including our three-pillared approach across prevention, protection and proactive and systemic change; how we deal with complaints made to eSafety; and how we engage with law enforcement partners, offenders and victim-survivors; can be found in our October 2022 submission to the Parliamentary Joint Committee on Law Enforcement inquiry into law enforcement capability in relation to child exploitation.

Technologies within the scope of the Bill

Anonymising software

The Bill seeks to amend Schedule 2 of the *Child Protection (Offender Reporting and Offender Prohibition Order) Act 2004* to require the possession or use of anonymising software to be reported as a personal detail by a reportable offender.

Anonymising software allows a user to hide or disguise their identifying information, such as their real name, age, location and data use. Examples include virtual private networks (VPNs) that mask the user's location and device details (such as their IP address) and programs that conceal the link between a message and the sender.

There are also simpler approaches to identity shielding which do not require software, including taking on a fictional identity, such as using a false name (a 'pseudonym' or an 'alias'), a virtual representation (an 'avatar'), or a fake profile. eSafety understands that existing legislation already requires offenders to report the details of any social networking site that they join, participate in or contribute to, including either the email address, username, or identity associated with an instant messaging service. This is important, given that anonymous offending can be perpetrated through such accounts without the use of any additional anonymising software.

eSafety emphasises that there are a number of legitimate reasons for shielding one's identity online, such as limiting or controlling how personal data is collected and accessed to prevent intrusive web-tracking, protecting vulnerable users from unwanted contact, and enabling people to freely engage online without feeling inhibited.

At the same time, identity shielding is one of several factors highlighted by our own investigations as a tactic used by those who seek to harm or abuse others online. There are two main reasons for this.

Firstly, being anonymous can make perpetrators feel uninhibited by the usual social standards of behaviour. By hiding their real identity or using fake profiles they can act without the fear of being judged for their actions or punished.

Secondly, being able to hide their real identity allows individuals and crime syndicates to pretend to be someone else and use that as a way to exploit others.

Interaction with an anonymous, pseudonymous or imposter account online can be very distressing for victims of sexual exploitation and other forms of abuse. The fear that the perpetrator can continue to target the victim using new accounts adds to the harm. Fake accounts can be quickly discarded and replaced with new accounts, making techniques such as reporting, blocking, muting and suspending accounts ineffective, and creating challenges for the identification and prosecution of those using fake accounts and identity shielding tactics.

Currently, online services are adopting a variety of mechanisms to detect, address, remove and report offenders to relevant authorities. However, our investigations have shown that offenders can bypass services' existing mechanisms and may use a variety of techniques to evade detection and hide their identities. Therefore, while requiring reportable offenders to report their anonymising software and social networking accounts is an important step, the online industry also has an essential role to play in preventing and addressing misuse.

Encryption software

We also note the Bill's proposal to amend Schedule 2 of the Act to include software that encrypts, or encrypts and hides, information as part of the reportable applications.

Like identity shielding, encryption has legitimate uses to protect privacy and security. It is primarily employed to keep data and transactions secure and to prevent data breaches and hacking. It allows safe communication where this may not otherwise be possible and is used to protect valuable information such as passport credentials.

While encryption has positive uses, there are significant risks, as identified by the Bill. Encryption can assist in serious harms by hiding or exacerbating criminal activities, including online child sexual abuse. Technologies that detect illegal material by proactively checking for known CSEM currently do not typically work on systems that use end-to-end encryption (E2EE). Because of this, E2EE can facilitate the exchange and proliferation of CSEM, perpetuating the abuse of victims and exposing survivors to ongoing trauma. We therefore welcome the Bill's inclusion of encryption software as reportable information.

We also note that, rather than requiring additional software, encryption is increasingly built into mainstream messaging services. eSafety is concerned that there is an emerging drift towards the adoption of E2EE without services performing a risk assessment and putting in place mitigation measures to reduce the risk that encryption will allow offenders to engaging in sexual exploitation of children. Popular messaging services such as WhatsApp and iMessage provide end-to-end encryption by default and Meta is scheduled to rollout default E2EE for all personal messages and calls in 2023. The National Centre for Missing & Exploited Children (NCMEC) estimates that more than half of its reports would cease to be possible if platforms implemented E2EE without appropriate safeguards for children.

In this way, as encryption can pose serious challenges to the detection and prosecution of grooming, exploitation and distribution of CSEM, we also emphasise the important role the online industry has to play in ensuring that their services – end to end encrypted or not – are safe for users, particularly children.

Support for the amendments as part of a broader response

In line with the risks identified above, eSafety supports the proposed amendment to insert item 15A into Schedule 2 of the Act to include anonymising software and encrypted services as personal details to be reported by a reportable offender.

We consider that law enforcement responses, including monitoring offenders' use of technologies, should form part of a broad, cross-sector, multi-faceted approach to online safety by industry, government and the general public.

We have called on tech companies, including those who provide encrypted services or allow anonymous or pseudonymous accounts, to commit to, and focus on, detecting illegal content and activity through greater investment in suitable and robust approaches. These protections should be built in from the design stage, not retrofitted once harm has been done.

We have also called for greater industry transparency about what proactive and preventative steps can and should be taken to safeguard and protect users from CSEM and reportable offenders. In August 2022, eSafety issued its first notices under the Basic Online Safety Expectations framework to Apple, Meta (and WhatsApp), Microsoft (and Skype), Omegle, and Snap, requiring them to outline the steps they are taking to address CSEM on their platforms. We are currently reviewing services' responses and will consider what information is appropriate to make public.

As recommended by the WeProtect Global Alliance, multi-agency approaches that share intelligence to manage reportable offenders should be adopted. We note that current information-sharing provisions will be extended to include the Department of Home Affairs, Australian Border Force and the Australian Federal Police. We also encourage consideration of how communication pathways can be improved between industry and government, including law enforcement agencies, to ensure risks can be detected and addressed as early as possible.

eSafety looks forward to continuing to engage with the Queensland Police Service as it reviews the Act to ensure it remains contemporary and continues to meet its purpose.