Privacy and Other Legislation Amendment Bill 2024

Legal and Constitutional Affairs Legislation Committee Inquiry

October 2024

Australian Government | eSafetyCommissioner

eSafety.gov.au

Contents

Introduction

eSafety welcomes the opportunity to make a submission to the Senate Standing Committee on Legal and Constitutional Affairs Legislation Committee on the *Privacy and Other Legislation Amendment Bill 2024* (the Bill).

We believe that online safety and privacy are distinct, but related, concepts that can be mutually reinforcing. Given this close intersection, eSafety supports the holistic and coordinated approach outlined in the Bill. We support increased transparency and accountability from online services about how they handle personal information, as well as greater empowerment for individuals to exercise choice and control over their data.

In making this submission, we note:

- These reforms form part of a broader privacy law reform agenda, which is being progressed in stages. As outlined further below, eSafety's enabling legislation is also being reviewed and updated to ensure it is fit for purpose.
- The Bill encompasses a broad range of measures. We have focused on measures with the most relevance and nexus to eSafety's role and remit. This is primarily the proposed:
    - Children's Online Privacy Code.
    - Doxxing provisions.

About eSafety

The eSafety Commissioner (eSafety) is Australia's independent regulator, educator and coordinator for online safety. We aim to safeguard Australians from online harms and to promote safer, more positive online experiences.

The *Online Safety Act 2021* (Cth) (Online Safety Act) sets out our legislative functions. Our regulatory approach comprises the three pillars of prevention, protection, and proactive and systemic change.

- **Prevention:** While eSafety acts as an important safety net for Australians online, our primary goal is to prevent online harms from happening in the first place. This work falls under our prevention pillar. Through research, education and training programs, we aim to build the capacity of Australians to interact safely online. We seek to provide

Australians with the practical skills and confidence to be safe, resilient and positive users of the online world, and to know where to seek help if issues arise.

- **Protection:** Where online harm does occur, eSafety offers tangible, rapid assistance. This work falls under our protection pillar. Our individual complaints mechanisms allow us to investigate and take action to remove certain types of content relating to four types of harm: cyberbullying of children, cyber abuse of adults, the non-consensual sharing of intimate images, and illegal or restricted online content.
- **Proactive and systemic change:** With the rapid evolution of technology, eSafety knows we need to be at the forefront of anticipating, mitigating and responding to online harms. This work falls under our proactive and systemic change pillar. This includes our powers to regulate digital platforms' broader systems and processes, including through the Basic Online Safety Expectations (BOSE) and industry codes and standards. It also includes our Safety by Design initiative, as well as our work anticipating and responding to emerging tech trends, opportunities and challenges.

These pillars reflect our broad and holistic remit underpinned by the functions under the Online Safety Act. The interoperability of these pillars reflects how eSafety's various functions work together to create a multidimensional regulatory toolkit.

We take a risk and harms-based approach to our work. We also recognise that combating online harm is a global challenge. We therefore work as part of a cross-sector and multi-jurisdictional online safety ecosystem. This approach is underpinned by our core mission of safeguarding Australians at risk of online harm and complements the role other agencies play in investigating and prosecuting crimes perpetrated online.

Statutory Review of the Online Safety Act

This submission draws from and refers to eSafety's current regulatory remit under the Online Safety Act.

As the Committee may know, an independent statutory review of the Online Safety Act is currently underway. This is to ensure it is an effective, up to date and future proofed legislative framework to protect Australians from online harms.

The Terms of Reference for the review are broad ranging and include consideration of eSafety's existing statutory schemes, including those outlined above. They specifically include consideration of:

- whether additional arrangements are warranted to address online harms not explicitly captured under the existing statutory schemes, and

- whether the regulatory arrangements, tools and powers available to the Commissioner should be amended and/or simplified, including through consideration of ensuring industry acts in the best interests of the child.

The Final Report of the review is expected to be provided to the Minister for Communications by 31 October 2024.

Children's Online Privacy Code

We support that the Bill proposes a Children's Online Privacy Code (COP Code) which would apply to online services that are 'likely to be accessed by children'. We consider the COP Code would be an important step in ensuring services are designed with the best interests of the child in mind, which strongly aligns with our own Safety by Design initiative.

We are pleased that the Information Commissioner is required to consult the eSafety Commissioner before registering the code. This will allow eSafety the opportunity to input our online safety experience and expertise into the COP Code's development.

Given the close relationship between privacy and online safety, this experience and expertise could include:

- Insights from our prevention, education and engagement work with young people, parents, carers and educators, among others.
- Insights and suggestions for industry from our Safety by Design initiative, including safeguards for children and young people that should be considered throughout the process of design, development and deployment.
- Insights from industry codes and standards under the Online Safety Act, including industry proposed safeguards for children and young people and regulatory requirements for specific industry sections.
- Insights from transparency requests under the Basic Online Safety Expectations, providing greater visibility of the about steps industry is taking to safeguard children and young people.
- Insights from eSafety research and engagement activities on specific online risks and how children's understanding of online safety and privacy evolves with age and development.
- Insights from eSafety's Youth Council, to ensure lived experiences and view of children and young people are considered.

We are also pleased to see that many aspects of the proposal promote regulatory coherence. Many of the terms defining the scope of the COP Code are also defined consistently with the Online Safety Act. This includes the types of providers covered and the definition of 'child'. The Basic Online Safety Expectations, also include an additional expectation that online service providers will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

Collaboration on the COP Code will be particularly important for regulatory coherence in relation to our own industry codes and standards, which cover intersecting issues and, in many cases, apply to the same group of stakeholders. There may be opportunities for practical benefits from regulatory coherence, such as in relation to complaints handling or information provision commitments.

As noted above, given the review of the Online Safety Act may change the contours of our legislation, the COP Code may need to mindful of any reform in order to maintain alignment.

Alignment with eSafety's industry codes and standards

eSafety has the power to register industry codes and develop standards spanning eight sections of the online industry including providers of social media services, relevant electronic services such as instant messaging, chat and gaming services, designated internet services including websites, providers of search engine services, app distribution, hosting, and internet carriage services, as well as equipment manufacturers. These phase 1 industry codes and standards are designed to protect Australians from illegal and restricted online content, by setting obligations for relevant industry sectors to proactively deal with this material at a systemic level.

The industry bodies tasked with developing the industry codes and standards adopted a two-phase approach. The first phase targets the most seriously harmful Class 1 material, which includes child sexual exploitation material, pro-terror material, and extreme crime and violence material. The second phase of industry codes development focuses on children's access or exposure to Class 2 material, which includes online pornography, simulated gambling and other high-impact themes.

eSafety is currently engaging with industry representatives on the development of the second phase of industry code development. The Phase 2 Codes Position Paper acknowledged the intersections between the Phase 2 codes and the proposed COP Code. It also outlined eSafety's intent to work closely with the Office of the Australian Information Commissioner (OAIC) to ensure codes both enhance safety and preserve privacy.

eSafety received interim draft codes from industry representatives on 3 October 2024. Final draft codes are due on 19 December 2024, following a public consultation. The eSafety Commissioner will then assess whether the code or codes submitted should be registered.

Six phase 1 industry codes are already in operation with two phase 1 industry standards set to take effect on 22 December 2024. Some phase 1 codes and standards contain compliance measures specifically in reference to children, because children face greater risks in relation to these harms. The Commissioner's decision on whether to register industry codes is based on whether they provide appropriate community safeguards for matters of substantial relevance to the community. This is informed by the best interests of children. One example of commonality between these codes and the proposed COP Code is privacy by default settings for children's accounts, which can help to protect both safety and privacy.

We welcome the opportunity to work with the Information Commissioner to align our approaches.

Alignment with the Basic Online Safety Expectations

Some of the Bill's proposals may also cross over with, and support, a provider's compliance with its online safety obligations. For example, the Basic Online Safety Expectations (BOSE) set out the Government's expectations that services are already taking reasonable steps to ensure users can use a service in a safe manner, such as making sure the default privacy and safety settings of services targeted at, or used by, children are robust and set to the most restrictive level.

We welcome and agree with the OAIC's submission to the consultation into the amendment to the BOSE determination, which stated 'the BOSE Determination will continue to facilitate an approach in which privacy and online safety are not mutually exclusive considerations but complementary components to address the risks and harms faced by Australians in the online environment'.

We note that some of the information we've gathered from services using our information gathering powers and requests under the BOSE may also be relevant to the OAIC. For example, we are currently working on a report relating to the number of children and current age assurance practices on services, which we'll release publicly.

Doxxing provisions

We support that the Bill proposes two new doxxing offences. As outlined further below, eSafety receives complaints that relate to doxxing and has observed the incredible harm it can cause.

The proposed offences would be criminal offences under the Criminal Code. They would cover the use of a carriage service to make available, publish or distribute personal data of one or more individuals, in a way that reasonable persons would regard as being menacing or harassing.

eSafety previously made a submission to the Committee on its inquiry into the *Criminal Code Amendment (Deepfake Sexual Material Bill) 2024.* Many of the broader points we made in that submission apply in this context as well, including that eSafety's whole of community and multidimensional regulatory remit complements and mutually reinforces a criminal justice response.

Below we outline how eSafety's investigative schemes can capture doxxing, as well as our broader work in this space.

eSafety and doxxing

Complaints and content removal schemes

eSafety operates four complaints schemes that investigate and can facilitate removal of content: cyberbullying of children, cyber abuse of adults, image-based abuse (which covers non-consensual sharing of intimate images), and illegal or restricted online content.

In our complaints schemes and our broader work, eSafety often sees the following types and dynamics of doxxing:

- Doxxing with the intention of intimidating, harassing or embarrassing, in the context of bullying or abuse.
- Doxxing as part of volumetric attacks, whereby it is the combination of a number of people sharing or accessing information that causes harm.
- Doxxing within the context of family, domestic and sexual violence.

Sources of identity and modes of oppression are often weaponised. This includes in relation to people and groups that form part of an at-risk group.

The majority of doxxing complaints are handled under our **Adult Cyber Abuse** scheme. Most notably, eSafety received 136 complaints of doxxing under our Adult Cyber Abuse scheme in the year to 4 October 2024. This is an increase from 91 complaints in 2023.

The threshold for the Adult Cyber Abuse scheme is that the relevant content must be intended to cause serious harm, as well as being menacing, harassing or offensive in all the circumstances. eSafety recognises that a broad range of online material and behaviour can be abusive and harmful even if it does not meet the legal threshold for adult cyber abuse.

We have also received 87 complaints about doxxing under our **Cyberbullying** scheme in the year to 4 October 2024, which applies to children. The threshold for the Cyberbullying scheme is that the relevant content must be intended to have the effect on an Australian child of seriously threatening, intimidating, harassing or humiliating. This is an increase from 42 complaints last year.

We sometimes approach online service providers informally to ask them to remove harmful material in the first instance where it may breach the platform's own terms of service, as this generally results in faster removal of material compared to formal actions. We have strong relationships with most major providers. This means we are usually able to facilitate rapid removal of harmful content, which can include information that identifies, locates or facilitates contact with complainants.

Every situation is unique and eSafety is committed to helping all Australians who seek our assistance with online harm. Where we find that material does not meet the threshold for our complaints schemes, eSafety will still try to help the person who made the complaint. This may include:

- providing tips and information for avoiding or minimising the impact of abusive material
- directing them to resources and other organisations or agencies that may be able to provide further support, and
- considering whether the material may have breached the terms of use of the online service provider and, if serious enough, informally requesting removal (even though the service is not obliged to take action).

We welcome that these offences may provide complainants with an alternative avenue for assistance through law enforcement. We also raise the need for clear communication and messaging to the public, which will help them understand where to go for help and the variety of options they have.

We already work directly with law enforcement where something appears to meet a criminal threshold or there is evidence that a person is under a real threat of physical

harm. This includes referring specific matters for criminal investigation. We have memoranda of understanding with policing organisations across the country to facilitate our engagement. This helps achieve a degree of coordinated, cross-agency and multi-jurisdictional effort.

Analysis of Bill

We provide some feedback on the doxxing provisions below. This is based upon our regulatory experience and insights outlined above. It is also in line with our objective of ensuring the provisions are capable of capturing, and are clearly expressed to capture, the types of doxxing eSafety sees, provided the relevant thresholds and criterion are met.

Personal data

eSafety is pleased to see that the definition of 'personal data' is broad, flexible and inclusive.

We offer some considerations below, consistent with the explanatory memorandum that notes that the offence is intended to be flexible. This is also intended to ensure the offences are consistent with a converged and modern media environment. In summary, we suggest in relation to the definition of personal data that:

- 'Online account' is intended to be interpreted broadly. This would ensure that a variety of online and digital platforms and services are captured.
- An 'image' may be 'still or moving'. This would clarify that it applies to video and other audio forms. This is a form of words used elsewhere in the Criminal Code and is consistent with the Explanatory Memorandum's statement that 'personal data' includes a 'photograph or other image'.
- It applies to real or natural versions of material, as well as computer-generated and AI-generated versions, including deepfakes.
- It applies to IP addresses, location information and other information that can reveal a person's identity.

Protected groups under the aggravated offence

The offence under proposed s 474.17D would apply in respect of people who the accused believes to be part of a group wholly or partly distinguished by one or more protected characteristics.

eSafety applies an intersectional lens to its work that recognises that diverse communities can be at greater risk of online harm. As noted above, we see online abuse is often based

on modes of oppression and multiple forms of prejudice, including sexism, misogyny, racism, ableism, homophobia, biphobia and transphobia.

Under our Adult Cyber Abuse scheme, eSafety must determine whether material meets the statutory threshold of being 'menacing, harassing or offensive' in all the circumstances. As our regulatory guidance explains, one factor that may be relevant in this determination is whether a person has been targeted because of their cultural background, gender, sexual orientation, disability, mental health condition or family, domestic and sexual violence situation.

There is a high level of correlation between eSafety's list of targeted reasons and the protected groups outlined in the Bill. However, we note that some at-risk groups may not be directly captured within the protected characteristics that define the offence under proposed s 474.17D. This includes victim-survivors of family, domestic and sexual violence. This is because the experience of family, domestic and sexual violence is generally understood as a circumstance or context for abuse, rather than a protected characteristic.

An example of where this may occur is if the identifying details of victim-survivors who form part of a support group are released publicly. It is therefore important that groups or cohorts that are at high risk but don't have a protected characteristic under proposed section 474.17D, such as victim-survivors of family, domestic and sexual violence, are captured under proposed under section 474.17C, which applies to individuals.

Conclusion

eSafety supports and welcomes the Bill, which demonstrates how privacy and online safety can be complementary components to address the risks and harms faced by Australians in the online environment.

We have a close relationship with the Office of the Australian Information Commissioner, as a fellow member of the Digital Platform Regulators Forum (DP-Reg) and look forward to continuing to work collaboratively.

Notably, the proposal for a COP Code demonstrates how measures to protect privacy can cross over with, and support, an organisation's compliance with its online safety obligations. We look forward to contributing our experience and expertise to the COP Code and ensuring online safety is embedded within, and supports, enhanced privacy for children.

We also welcome greater recognition of how serious doxxing can be. Noting that eSafety's civil schemes work in a complementary manner to criminal justice responses, we anticipate that the new offences may provide complainants with an alternative avenue for enhanced

assistance through law enforcement. We note again the need for clear communication and awareness raising with the public to help them understand where to go for help and the variety of options they have.