Australian Government | eSafetyCommissioner

Consultation for Online Privacy Bill

eSafety submission

December 2021

Introduction

Despite misconceptions to the contrary, safety, privacy and security are complementary, not contradictory, concepts.

The eSafety Commissioner (eSafety) believes it is possible to identify and respond to serious online harms, while still maintaining strong security of systems and protecting privacy.

But while safety, privacy and security issues are closely intertwined, care must be taken to not conflate or confuse the objectives that each discipline is seeking to achieve.

The *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (Online Privacy Bill) raises important issues and eSafety welcomes the opportunity to make a submission: to comment on the issues relating to children's online privacy and digital participation; and to explain related areas of work that we are undertaking, particularly the development of an age verification roadmap which is due to be delivered to the Australian Government in December 2022.

eSafety also welcomes the fact that the eSafety Commissioner must be consulted and her views regarded as part of deciding whether to register the Online Privacy Code.

As the stakeholders engaged in our age verification (AV) consultations have raised with us, it is essential that any approach to AV or age assurance (AA) is proportionate, viable and privacy- and security-preserving. Otherwise, implementation may undermine, rather than enhance, privacy.

More broadly, it is important to be clear about the problem any regulatory intervention is trying to solve to ensure reasonable, proportionate and effective solutions are identified.

Indeed, it is important to coordinate regulatory schemes to minimise overlap, confusion and inconsistency to the greatest extent possible.

Consistent with the United Nations Convention on the Rights of the Child to which Australia is a party, the rights of the child must be of paramount consideration in any process affecting them.

While we note the importance of protecting children's data, we consider it may run counter to the rights of children if a consequence of the Online Privacy Bill was to prevent children from accessing the vast benefits of social media.

Overview

In this submission, eSafety outlines its workstreams that intersect with the Online Privacy Bill, particularly AV and AA measures that are currently under consideration for social media and other online services.

Given the synergy between safety, privacy and security, a particular focus of this submission is the process and implementation challenges that may arise if the code under the Online Privacy Bill is implemented.

We note that the AV provisions within the Online Privacy Bill were not specifically included in the Australian Competition and Consumer Commission's Digital Platforms Inquiry report that recommended the Office of the Australian Information Commissioner develop a privacy code for digital platforms.

We also note we have raised some of these matters in other consultation processes for the Online Privacy Bill. We have welcomed the constructive manner in which our feedback has been received and are hopeful it will be reflected in the next iteration of this process.

eSafety

eSafety is Australia's national independent regulator for 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.

We draw upon social, cultural, technological and regulatory initiatives and interventions. Through the key pillars of protection, prevention and proactive and systemic change, eSafety's aim is to minimise harm online.

eSafety undertakes an extensive research program to ensure its programs and resources are evidence based.

Our research is supplemented by insights from our policy work, education and outreach programs, investigative teams and extensive community outreach.

Overview of Online Safety Act

On 23 January 2022, the new *Online Safety Act 2021* (Cth) (Online Safety Act) will commence.

The Online Safety Act will expand eSafety's regulatory remit and my functions and powers as eSafety Commissioner, improving the effectiveness, reach and impact of eSafety's work.

It establishes a world's first complaints and investigations scheme for Australian adults who experience serious cyber abuse online. It will also expand the cyberbullying scheme for Australian children, enabling eSafety to require the removal of material from the full range of online services where children are now spending time, not just social media sites.

Importantly, the Online Safety Act also includes a number of measures that will seek to make platforms and services safer. Of note, eSafety's remit includes:

- Promoting and assessing the compliance of services, including social media services (SMS), with the new Basic Online Safety Expectations (BOSE), which include expectations to:
    - ensure safe use, for example, by ensuring that default privacy and safety settings of services used by children are robust and set to the most restrictive level, and
    - have measures in place to prevent children's access to class 2 material (such as pornography), for example, by implementing age assurance mechanisms.
- Registering codes for 8 sections of the online industry, including SMS, which will among other things:
    - contain measures to prevent children from accessing class 2 material, such as pornography, including the use of age assurance or verification mechanisms, and
    - see codes relating to class 1 material (such as child sexual exploitation material and pro-terror content) registered by July 2022 and codes relating to class 2 material (such as pornography) registered by December 2022, if eSafety's recommended phased approach is adopted.[1]
- Drafting and registering a new Restricted Access System Declaration, a legislative instrument defining the features that must be present in any mechanism intended to limit access to restricted material online. eSafety will have the power to issue a notice to SMS and other online services

[1] eSafety has recommended this phased approach to align with the timing of its age verification roadmap, which is due to be delivered to Government in December 2022. If industry chooses not to pursue a phased approach, codes covering the full range of issues, including age assurance or verification measures for class 2 material, are expected to be registered by July 2022.

provided from Australia requiring them to place certain class 2 content behind a Restricted Access System to prevent children's exposure.

In addition, eSafety is seeking to expand its technical capability and knowledge to ensure we stay at the leading edge of developments in online safety technologies. Through our safety tech work, we will endeavour to provide robust, data-driven, evidence-based and objective overviews, assessments and evaluations of online safety innovations, technologies and products. Consistent with stakeholder feedback on the importance of consumer choice and offering safety solutions across multiple layers, this will extend beyond AV and AA technologies and encompass additional options to promote children's safety online, such as device-level filters and parental controls.

Age verification and assurance concepts

Age assurance (AA) is an umbrella term that captures age verification and age estimation technologies. The objective of AA is to accurately test, assess or confirm someone's age. Measures to achieve this include age-gating, age estimation or prediction, biometrics, behavioural or signal analysis, as well as verification through official documentation or identity systems.

AV is a process that relies on verified sources of identification to provide a high degree of certainty for the age of a user. It is often coupled with 'liveness' or 'real-time' tests. AV uses 'hard identifiers' to determine proof of age, through the extraction of age attributes from official documentation, such as passports, photo ID or healthcare number.

Age estimation is a process that establishes whether a user is likely to be of a certain age or age range. Estimation can be undertaken using real-time biometrics, such as facial analysis, keystroke dynamics, voice, finger or palm prints. It can also be undertaken with user profiling, including how they engage on a platform, the age of their contacts and age-range of their interests or groups.

Existing work going on in this space

There is work underway on online verification systems across the Commonwealth.

The Digital Transformation Agency is progressing its work on a digital identity system.

The Australian Communications and Media Authority is creating a National Self-Exclusion Register for gambling.

As noted above, eSafety has been tasked with developing an AV roadmap for online pornography by December 2022.

By way of background, in February 2020, the Standing Committee on Social Policy and Legal Affairs finalised an inquiry into AV for online wagering and online pornography. One of its recommendations was to task eSafety with developing a roadmap to lay the necessary groundwork for a successful AV regime. The Senate Committee report specifically noted that a successful AV regime would require robust privacy, safety and security standards, a legislative basis, the consideration of complementary non-technical solutions and, importantly, understanding and acceptance among the community.

Bringing the public along on the journey and assisting them to understand these technologies and how data is used was identified as critical in the Senate Committee's report. Lack of public consultation and

subsequent lack of public support was found to be a key reason for the United Kingdom abandoning its original AV mandate.[2]

The need to raise awareness and support for AV is supported by eSafety's research with Australian adults, which showed that awareness of AV is not high (around 50%).[3] Further, around a quarter (24%) of respondents lacked confidence in the effectiveness of its design, implementation and operationalisation by government.

This is why, in part, the Australian Government has asked eSafety to conduct a thorough consultation and develop a roadmap to lay the foundation for a workable AV regime to protect children from exposure to pornography.

The AV roadmap process includes research and consultation on proportionate AV and AA measures to ensure recommendations are privacy preserving and offer data security. There are international standards and technical requirements currently in development for AV and AA technologies, which eSafety will draw upon in drafting our report.

eSafety has until December 2022 to deliver the roadmap to ensure sufficient time to consult with industry, stakeholders and the public. This time is necessary to ensure AV options are underpinned by a robust evidence-base and partnered with extensive community consultation.

This process began in August 2021 when eSafety issued a call for evidence seeking insights into effective AV and AA techniques, as well as the impact of online pornography on children and proven methods of educating young people about both respectful and harmful sexual behaviours. We have published a high-level thematic analysis of the evidence emerging from this first phase of input on our website.[4] This analysis canvasses many of the key issues relating to risk, proportionality, effectiveness and the need for holistic approaches that are of key relevance to the Online Privacy Bill.

These submissions have informed the next phase of targeted consultation, which commenced in November 2021 to allow closer examination of the themes that emerged from the call for evidence. We are still in the early stages of the consultation process, and there will be more opportunities to contribute early next year for those who are yet to be involved.

Following the consultations, eSafety will continue to work closely with relevant stakeholders to define the minimum requirements for an effective regime and scope its various elements. These requirements and elements will then be presented to the Australian Government for consideration at the end of 2022.

There is significant benefit in leveraging the findings from this roadmap, particularly given the extensive research and consultation that has informed the process and will continue to guide its development.

It is our view that a separate AV or AA process at the same time would be onerous, duplicative and confusing for industry and consumers, particularly given the close intertwining of privacy and safety issues on social media. This has also been voiced by stakeholders engaged in our consultations, who have welcomed the extensive consultation and engagement process eSafety is undertaking.

---

[2] In May 2021, the UK government released the Online Safety Bill 2021 (UK), which includes the requirement that if a platform can accessed by children, it will have to comply with the safety duties for child protection. It also imposes duties of care in relation to content that is harmful to children, such as pornography. Age-verification is one of many measures that companies in scope may be required to implement to protect children from inappropriate content...

[3] eSafety, Public perceptions of age verification for limiting access to pornography, October 2021, https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography

[4] https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification

For this reason, eSafety strongly recommends close coordination and harmonisation of AV or AA expectations, standards, recommendations and requirements being developed under the age verification roadmap, the Online Safety Act and the Online Privacy Bill. This alignment of government processes is likely to address risks of duplication and confusion.

There are some key variances between the schemes that may affect their interoperability, which we outline below and encourage be given further consideration.

Promoting consistency

eSafety encourages a coordinated and consistent approach between the Online Privacy Bill and overlapping measures under the Online Safety Act. We believe an aligned framework for age-appropriate design, with consistent definitions, would be more effective for public and industry understanding, implementation and enforcement.

Definitions

The definition of SMS in the proposed Online Privacy Bill differs from the definition under the Online Safety Act.

Under the Online Privacy Bill, a SMS is an electronic service that has the sole or primary purpose of enabling online social interaction between two or more end-users, and allows interactions between end users, and allows end-users to post material on the service.

Under the Online Safety Act, an SMS is defined in a similar way, but exempt from its definition are relevant electronic services (RES) and designated internet services (DIS), which are defined separately. However, some RES and DIS would be included in the definition of SMS under the Online Privacy Bill. For example, the explanatory paper for the Online Privacy Bill notes that online messaging platforms and interactive games are a SMS, whereas they would be a RES under the Online Safety Act. We outline the practical challenges to this below.

Industry associations are currently drafting the codes to be registered under the Online Safety Act. At present, it is not clear whether there will be separate codes for SMS, RES and/or DIS, or if these three sections of the online industry will be grouped under a single code. In our position paper to guide the development of codes, eSafety has expressed the view that an approach which results in fewer codes is likely to be most effective and efficient.

Given many digital platforms will be subject to both safety and privacy codes, there is a risk it would create regulatory inconsistency and confusion, if a service is categorised as a SMS for one code and a RES for another. A more harmonised definition is likely to lead to greater compliance from industry and result in greater take up and support from Australian consumers. This was something we raised in earlier consultations and unfortunately, was not taken on-board.

Penalties

In addition, the penalties under the Online Privacy Bill and Online Safety Act differ, with the maximum penalty under the Online Privacy Bill for an individual being 2,400 penalty units, while it is 500 penalty units under the Online Safety Act.

The penalties under the Online Privacy Bill may be considered disproportionate and punitive in light of the Online Safety Act. The disparity may also lead to some participants prioritising compliance with the Online Privacy Bill, given the significantly greater penalties associated with non-compliance, whereas a high standard of compliance among both schemes is ideal. These penalties need to be proportionate and

consistent and there is little information available as to how the quantum of these high penalty units were arrived at.

Areas for further consideration

We outline below aspects of the Online Privacy Bill that we encourage be given further consideration to ensure any adverse impacts are mitigated.

1. Exclusion of those who unable to verify their age (16+) or parental consent (under 16)

The Online Privacy Bill will require SMS to take all reasonable steps to verify the age of end-users and obtain parental consent before collecting, using or disclosing personal information of children under the age of 16 years, and take all reasonable steps to verify the consent.

Mandating that no personal information may be collected from those who cannot verify that they are aged 16+ or obtain parental consent may have inadvertent adverse effects. The risk is particularly acute for at-risk children.

Children who cannot obtain parental consent or establish their age may be excluded from the benefits of online services. This includes connection to friends, family, culture, education and entertainment. This may also create barriers to their ability to access important information and services, including health and wellbeing services, and have significant negative mental health effects.

Notably, Australian young people experiencing psychological distress are more likely to use social media as a source of support than young people not experiencing psychological distress.[5]

As outlined in the United Nations General Comment on children's rights in relation to the digital environment:

> 'Meaningful access to digital technologies can support children to realize the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.'[6]

It is important to understand the potential detrimental impacts of limiting children's engagement through a blunt force requirement, as improvements to privacy should not have the effect of eliminating the many benefits of online participation.

While eSafety research suggests that children whose parents and carers use restrictive measures are less likely to be exposed to harmful content online (54% compared to 64% of children whose parent do not restrict their internet use), findings also suggest that this can hinder the ability of children to use the internet in more meaningful and positive ways.[7] Children whose parents place restrictions on their online activities are much less likely to use the internet for schoolwork, to learn, to seek information and to meet and interact with others.

These emerging insights are broadly consistent with international evidence that children who receive restrictive mediation from their parents are much less likely to engage in diverse activities online, including informational and creative activities.[8]

---

[5] Hall, S., Fildes, J., Perrens, B., Plummer, J., Carlisle, E., Cockayne, N., and Werner-Seidler, A. (2019) Can we Talk? Seven Year Youth Mental Health Report - 2012-2018. Mission Australia, Sydney

[6] United Nations, Committee on the Rights of the Child, General Comment on children's rights in relation to the digital environment, March 2021, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=en

[7] eSafety, Ref. Early release of headline findings, November 2021, https://www.esafety.gov.au/newsroom/media-releases/australian-young-people-learning-push-back-against-online-bullies

[8] Global Kids Online (2019). Global Kids Online: Comparative Report, UNICEF Office of Research – Innocenti. page 42.

Australian privacy laws to date have not specified an age after which individuals can make their own privacy decisions. As a general rule, an individual under the age of 18 has the capacity to consent when they have sufficient understanding and maturity to understand what is being proposed.[9]

This links to an important point that when considering children's rights, the evolving capacities of children should be a core consideration.

However, to our knowledge, there has not been an independent evaluation of the capacity of children at various ages to make an informed decision to provide personal data to an online service provider. While the General Data Protection Regulation sets the default age at which a person is no longer considered a child at 16, we understand that it allows member states to adjust that limit to anywhere between 13 and 16 and countries across the European Union have chosen different ages within that range.

It is also important to note that children will differ in how their capacity evolves: a 14-year-old may have more maturity and the ability to make decisions than a 16-year-old. Mandated and specific age restrictions can become arbitrary, and exclusionary, in this context.

While we note that the requirement is for services to take reasonable steps to verify the age of end-users and obtain parental consent, it is unclear how this would apply in practice. We explore this further below.

Importantly, the online world offers innumerable benefits to children and young people. While parental discretion should be supported, it should not be prioritised over the needs of children. Consideration should also be given to whether parents and carers have the knowledge and support to make informed decisions about their children's privacy and safety.

It is imperative that we balance the rights of children to participation, inclusion and privacy with their right to protection and safety in digital environments.

In addition to the unintended consequences of parental consent measures, there are privacy implications of requiring all Australians to verify their age and consent to use a SMS.

2. Requiring the collection of additional personal information

Given that a core privacy principle is the importance of data minimisation, it may seem incongruent to have age and parental consent verification measures within a law reform process based on privacy protection.

Some services may not currently have the systems, processes and technologies in place to enable them to collect and maintain consent verification data in a privacy- and security-protecting manner.

From our experience with SMS, it is unclear whether services have the knowledge and capabilities to understand and consistently apply a reasonable steps criterion, which may therefore become challenging to implement.

Before these measures are put into place, it is important to test services' capacity to implement appropriate systems and to promote public understanding and trust that such systems will serve to enhance, rather than undermine, children's privacy, as well as the privacy of all Australians.

It is precisely these complex policy, process and implementation issues that eSafety's AV roadmap will explore.

[9] OAIC, APP Guidelines, Chapter B, Page 13: https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

3. Limitations of age verification or assurance

AA or AV is an important safety step. However, it is only the first step. It is imperative to consider what the most appropriate 'next steps' are once a user's age is estimated or verified in order to promote their safety and privacy. Put simply, on its own and without broader safety interventions and initiatives, AA or AV do not enhance privacy or safety.

If the only obligation after verifying or estimating that a user is a child is to obtain parental consent, this obligation can be discharged without services having to apply any increased privacy or safety protections to the accounts of those children who received permission. This may create a false sense of security for parents and guardians who provide consent believing that services are taking steps to keep their children safe online simply by using AV.

Examples of safety interventions which could be imposed after ascertaining that a user is a child include imposing high default privacy and safety settings, as will be expected under the BOSE in the Online Safety Act.

As such, if there are additional obligations in relation to default privacy and safety settings, it is important they align with eSafety's measures under the codes and the BOSE.

4. At-risk and vulnerable groups

The Online Privacy Bill defines vulnerable groups as people who are physically or legally incapable of giving consent to the collection, use or disclosure of personal information

We raise two aspects of this definition for further consideration. Firstly, similar to our comments above, a potential unintended adverse consequence is that this could lead to vulnerable people being excluded from the benefits of online services, which may be both exclusionary and discriminatory. We would support an approach that seeks to build vulnerable users' capacity to understand what they are signing up to when they engage on SMS and to empower their safe, private and secure use through appropriate settings, tools and other measures.

Secondly, this definition may not recognise that a broader range of at-risk groups may be at disproportionate risk online.

eSafety's research and experience points to the fact that online harms can disproportionately impact at-risk and diverse groups. This includes, but is not limited to, Aboriginal and Torres Strait Islander people, people from culturally and linguistically diverse communities, people with disability and people who identify as LGBTQI+, as well as, depending on the circumstances, women, older people and children and young people.

To be clear, we are not suggesting these groups lack the capacity to make their own safety or privacy decisions. Rather, we are saying risk online is complex and includes an appreciation of structural and systemic issues, including social modes of oppression, such as sexism, racism, ableism, ageism, homophobia and transphobia.

There is a risk that the definition for vulnerable groups does not appreciate that online harms exist on a continuum, in which capacity is only one relevant factor. The focus should not be on excluding anyone from interacting online, but giving them the support they need to engage online safely.

Safety by Design

As outlined above, obtaining parental consent for children to use SMS will not, on its own, protect children's privacy or safety.

A multifaceted approach is needed.

eSafety also has a world-leading Safety by Design (SbD) initiative. It encourages technology companies to anticipate, detect and eliminate online risks as the most effective way to make our digital environments safer and more inclusive, especially for those most at-risk, including children.

In addition to applying AA or AV at sign-up, a layered, proportionate and effective SbD response to protecting children online could include:

- Setting rules for users' minimum age and/or age limits, where appropriate.
- Detecting and preventing or removing users outside of that age range.
- Making services safe, private and appropriate for users within that age range. This could include:
    - higher default safety and privacy settings for younger users,
    - provision of tools and controls to help users manage who, what and how they interact with others, and
    - limiting or providing controls to manage the type of content that is promoted to or accessible by children.

The next phase of the SbD initiative will focus on ensuring the needs of diverse and at-risk groups are effectively considered, incorporated and actioned within SbD. We'll be engaging with at-risk groups through sessions for this purpose.

Capacity building

Regulation is important, but it only one part of a multifaceted response.

AA and AV do not provide children, or their parents and carers, with the safety skills and strategies they need to navigate safely online.

This is why eSafety focuses on digital capacity building: giving individuals the skills and strategies to prevent and respond to harmful experiences online and engage online in ways likely to promote safe and positive online experiences.

Capacity building should be a lifelong process that begins at the earliest age possible.

eSafety has an extensive education and outreach program to support this stream of work. The four Rs of online safety — respect, responsibility, resilience and reasoning — are a basis for examining online information and making an informed judgement on an issue. eSafety has also developed a Best Practice Framework for Online Safety Education based on an evidence review. The review found that a sound online safety education should cover the full range of potential issues, risks and harms that children may encounter and should be delivered in supportive school systems with strong partnerships with other agencies.

Encouragingly, our recent youth survey showed most children and young people are taking action in response to nasty or hurtful behaviour online, suggesting that they have gained the digital skills and self-efficacy to address these experiences.[10] For example:

- 93% of children did something in response to a negative online interaction

[10] eSafety, Ref. Early release of headline findings, November 2021, https://www.esafety.gov.au/newsroom/media-releases/australian-young-people-learning-push-back-against-online-bullies

- 67% told their parents about the incident
- 63% unfriended or blocked the perpetrator (63%)
- 61% told their friends (61%)
- 55% tried to get the other person to leave them alone
- 50% deleted any messages from the person
- 41% changed their privacy or contact settings

Also encouragingly, in comparison to research eSafety conducted in 2017, analysis indicates increases in young people taking action to address and prevent bullying and other hurtful behaviours from 2017 to 2021.

There is also evidence that young people actively curate their social media feeds and self-regulate their social media use to maximise positive and minimise adverse effects.[11]

This demonstrates the importance of giving young people tools and techniques to navigate online safely, in addition to skills and strategies for responding to harm, risk and negative experiences online.

Crucially, children gain experience and resilience from navigating online, which then becomes a protective factor for their future online experiences.

eSafety also has a suite of resources for parents, guardians, teachers and the community to give them the knowledge, skills and support they need to assist the children and young people in their lives interact online safely.

Conclusion

In closing, we want to reiterate the importance of a multifaceted approach, which promotes consistency across the regulatory spheres of safety, privacy and security, especially in relation to process and implementation.

With any intervention that seeks to protect children, the problem must be clearly identified, the solution reasonable, proportionate and effective and the rights of the child paramount.

We are happy to provide any further information and look forward to continuing to work constructively on this process.

11 Rideout, V. & Fox, S. 2018, Digital health practices, social media use, and mental wellbeing among teens and young adults in the USA, A national survey sponsored by Hopelab and Wellbeing Trust