Roadmap for age verification

and complementary measures to prevent and mitigate harms to children from online pornography

March 2023

Australian Government | eSafetyCommissioner

eSafety.gov.au

About eSafety

The eSafety Commissioner (**eSafety**) is Australia's independent regulator and educator for online safety. eSafety promotes online safety for all Australians, leads online safety efforts across Australian Government departments and agencies, and works with online safety stakeholders around the world to extend our impact across borders. Established in 2015, our mandate is to make sure Australians have safer and more positive experiences online.

Acknowledgment

eSafety acknowledges all First Nations people for their continuing care of everything Country encompasses — land, waters, and community. We pay our respects to First Nations people, and to Elders past, present, and future.

Contents

About eSafety 2
Acknowledgment 2
Contents 3
Overview 5
Summary of key findings, proposed next steps and recommendations 7
If and how a mandatory age verification mechanism or similar for online pornography could practically be achieved in Australia 7
A suitable legislative and regulatory framework 9
Complementary measures for a holistic approach 11
Activities for awareness raising and education 14
Mandatory age assurance mechanism 16
Background 16
Global and industry developments 17
Public perceptions and important factors 18
Findings from the independent assessment 19
Age assurance requirements and expectations under existing regulations 21
Evidence to inform such a mandate 22
Coordination with the National Plan 26
Remaining gaps in evidence 26
eSafety's proposed next steps 27
Recommendations for the Australian Government 27
Legislative and regulatory framework 30
Online safety regulatory framework 30
Online Safety Act 30
Classification, removal, and remedial powers 30
Industry codes and standards and service provider determinations 32
Basic Online Safety Expectations 32
Compliance and enforcement 34
Privacy, security and governance regulatory framework 35

eSafety's proposed next steps 38
Factors that could be considered as part of the forthcoming independent review of the Online Safety Act 39
Additional factors to consider for an age assurance pilot 40
Complementary measures and a holistic approach 41
Background 41
Experiences of under 10s and relevant complementary measures 42
Experiences of 10-13-year-olds and relevant complementary measures 44
Experiences of 13-15-year-olds and relevant complementary measures 47
Experiences of 16-17-year-olds and above and relevant complementary measures 50
eSafety's proposed next steps 54
Education and awareness raising 57
For parents and carers 58
For educators 60
For frontline workers and others working with children 62
For children and young people 63
The needs of diverse communities 65
Need for consistency, flexibility, and coordination 66
Public awareness to support the implementation of age assurance 69
eSafety's proposed next steps 70
Recommendations for the Australian Government 71
Consultation 72
Roadmap 72
Appendix A: 73
Recommendations for the Australian Government 73
Appendix B: 75
Consultation participants 75
References and notes 77

Overview

Beginning in 2019, the House of Representatives Standing Committee on Social Policy and Legal Affairs (**the Committee**) conducted an inquiry into age verification for online wagering and online pornography (**the Inquiry**).

The Committee recommended the Australian Government direct and adequately resource the eSafety Commissioner (**eSafety**) to develop a roadmap for the implementation of a regime of mandatory age verification for online pornography (**the roadmap**), setting out:

- a suitable legislative and regulatory framework
- a program of consultation with community, industry, and government stakeholders
- activities for awareness raising and education for the public
- recommendations for complementary measures to make sure age verification is part of a broader, holistic approach to address risks and harms associated with the exposure[1] of children and young people to online pornography.

The then-Australian Government supported the recommendation, noting the roadmap should be based on detailed research as to if and how a mandatory age verification mechanism or similar could practically be achieved in Australia.

To inform this work, eSafety:

- conducted a call for evidence and held extensive multi-sector consultations, summaries of which are available online
- undertook both desktop and primary research, including a survey and focus groups with participants aged 16-18, supported by further discussions with the eSafety Youth Council
- commissioned an independent assessment of age assurance and online safety technologies from Enex Testlab[2]
- consulted with relevant agencies and departments across government.

The methodology, results and broader context of these processes are explored in detail in a background report.[3] This roadmap is a high-level summary of eSafety's analysis and findings. Following each section of the report, we set out:

- proposed next steps for eSafety
- recommendations to the Australian Government
- any suggested relevant factors to consider as part of the forthcoming independent review of the *Online Safety Act 2021* (Cth) (**the Act**).

The roadmap reflects the guiding principles derived from our stakeholder consultations:

1. take a proportionate approach based on risk and harm

2. respect and promote human rights

3. propose a holistic response that recognises the roles of different stakeholders and supports those most at-risk

4. ensure any technical measures minimise data and preserve privacy

5. consider the broader domestic and international regulatory context

6. consider what is feasible now and anticipate future environments.

Summary of key findings, proposed next steps and recommendations

A complete list of the recommendations for the Australian Government can be found in **Appendix A**.

If and how a mandatory age verification mechanism or similar for online pornography could practically be achieved in Australia

Key findings

- eSafety's research with 16-18-year-olds found 75% of participants had seen online pornography. Of those, nearly one third saw it before the age of 13, and nearly half saw it between the ages of 13 and 15. The broader evidence base about the potential impacts of online pornography on children is complex and conflicting, and more research is needed to address existing gaps and limitations in the literature.
- While online pornography and children's experiences with it are not homogenous, studies point to a common and readily accessible 'mainstream' form of pornography. This material can be characterised as targeting a male heterosexual audience, may often contain depictions of sexual violence and degrading sexual scripts about women, and forming a significant proportion of the global online pornography market. It can be difficult to disentangle the potential impacts of online pornography from the broader context in which it is situated, however, there is research pointing to an association between mainstream online pornography and harmful sexual attitudes and behaviours.
- Age assurance[4] on its own will not address this issue. There are several reasons for this, including that many relevant studies point to an association between adult (18+) consumption of pornography and gender-based violence. However, to the extent that age assurance can serve to increase the age at which children encounter online pornography, making it more likely they are equipped with the critical reasoning skills and context to interpret what they are seeing, it can serve as a key component of a holistic response to preventing and mitigating this harm.
- Australia is not alone in exploring age assurance for various harms. Countries are at different stages of considering and implementing measures. As a result, the online industry is increasingly adopting more robust approaches beyond asking users to self-declare their age. However, significant gaps remain.
- According to eSafety research, more than three in four Australian adults support government implementation of age assurance for online pornography. However, there are concerns about effectiveness, privacy, and security. These themes – and concerns about accessibility, fairness and bias – were echoed by young people and multi-sector stakeholders.

- These considerations informed the development of assessment criteria which an independent test lab applied to review age assurance technologies available on the market, including biometric (age and voice) estimation and identity document (ID)-based tools. They also reviewed a recent European age assurance pilot and international standards for age assurance.
- The independent assessment found the age assurance market is immature but developing. Each technology has benefits and trade-offs. For example, ID-based solutions can provide a high level of certainty but risk excluding those without access to ID, whereas facial estimation technology is promising but may offer a lower level of certainty, and may vary in accuracy based on skin tone, gender, and physical differences. Consumer choice to select the option users are comfortable with, and which works for them, is a key lesson from the European pilot.
- For these and other reasons explored below, age assurance technologies should be trialled in Australia, based on lessons from pilots conducted elsewhere, before being mandated. While eSafety should be involved in the development, implementation, and evaluation of any such pilot, we do not presently have the resources, capabilities, or expertise to lead its delivery.

Next steps and recommendations snapshot (see page 27 for full details)

eSafety:

- Continue cross-government collaboration with activities relating to mainstream online pornography as a contributor to harmful gender stereotypes.

Australian Government:

- Fund specialist research examining the experiences with and impacts of online pornography with specific groups of children who are under-represented in existing literature.
- Trial a pilot before seeking to prescribe and mandate age assurance technology, informed by the considerations set out below.

A suitable legislative and regulatory framework

Key findings

We suggest there are two parts to the relevant legislative and regulatory framework.

- The first part would establish the expectations and requirements for service providers within the online industry to apply age assurance and other complementary measures to prevent, or limit, children's access to online pornography. The *Online Safety Act* can help fulfill this component, as the existing Australian framework for promoting online safety and seeking to regulate online access to such content. The Act and its subordinate legislation contain existing requirements or expectations for some online services to apply age assurance or other measures to prevent children from encountering high impact material such as online pornography. This includes the *Online Safety (Restricted Access Systems) Declaration 2022* (Cth) and the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth). Industry codes or industry standards to prevent children's access to this type of material will also be developed for eight sections of the online industry, in accordance with the requirements in Part 9 of the Act.
- The Minister is to initiate an independent review of the Act by January 2025, providing an important opportunity to consider potential issues for reform identified in the process of developing the roadmap. This includes lessons learned from the challenges other regulators have encountered in enforcing age assurance requirements in other jurisdictions.
- The second part of the legislative and regulatory framework would establish a regulatory scheme for the accreditation and oversight of age assurance providers, to promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights. Based on our consultations across government, at this stage, there is likely no existing regulator or accreditation body that has the full breadth of experience and capability to provide all the necessary functions.

- However, there is substantial work well underway to develop an equivalent regulatory scheme for Australia's Digital Identity System, led by the Digital Transformation Agency. In addition, the Attorney-General's Department's Privacy Act Review Report puts forward a range of proposals designed to ensure Australia's privacy framework responds to new challenges in the digital era. The Australian Government could build on this work – as well as relevant international standards – as the basis for a regulatory accreditation and oversight regime for age assurance. This discovery process could take place alongside the development and execution of an age assurance pilot, to increase Australia's readiness to implement mandatory age assurance should the pilot prove successful.
- In addition to developments in relation to the Digital Identity System, there are many other relevant government strategies, inquiries, plans, and legislative proposals underway in relation to privacy, security, human rights, and competition and consumer rights – some of which have a particular focus on biometric technologies (such as those which conduct facial age estimation). These initiatives straddle multiple portfolios, departments, and agencies – all of which should be engaged in the development, evaluation, and potential mandatory implementation of an age assurance pilot.

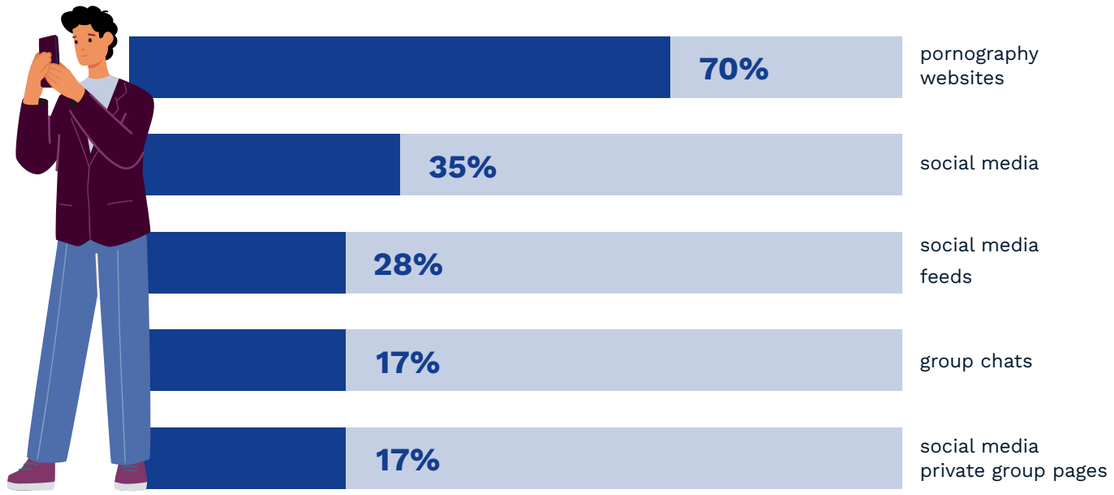
Next steps and recommendations snapshot (see page 34 for full details)

eSafety:

- Continue implementation of the Act, including the Basic Online Safety Expectations and Industry Codes or Standards, informed by the roadmap.
- Contribute to the review of the Act, advising on the suitability of existing regulatory powers to address children's access to online pornography.
- Continue cross-government collaboration on intersecting initiatives and reforms.

Australian Government:

- Implement cross-government stewardship in consideration of a pilot.



Contexts and places in which children encounter online pornography (both intentional and unintentional)

Complementary measures for a holistic approach

Key findings

- A holistic approach needs to consider the contexts and places in which children encounter online pornography. eSafety's research shows this includes both intentional and unintentional access, occurring across pornography sites (70%), social media feeds (35%), ads on social media (28%), social media messages (22%), group chats (17%), and social media private group/pages (17%).
- Online services' efforts to ascertain their users' age are only beneficial if accompanied by complementary measures to create a safe and age-appropriate experience for them. Different complementary measures may be suitable for children of different ages and developmental stages.
- A combination of supervision, safety discussions and the use of filters, safety settings, and parental controls can be highly effective at preventing younger children from encountering online pornography. However, parents and carers need support to access, understand, and apply these measures. Barriers can include cost, low awareness or digital literacy, and inability to calibrate settings. The online industry and government both have a role to play in assisting parents and carers to overcome these barriers.
- These measures can also be applied for older children. However, as children grow up, it becomes more likely they will be able to bypass filters and parental controls if they want to do so.

- Children between the ages of 10 and 12 may have less supervision than younger children and may seek to join social media and other online services intended for children who are 13 and older. Accordingly, it is important for those online services to take reasonable steps to prevent underage users from joining and to detect those who do manage to join. Search engines, app stores and other sections of the online industry are also important gatekeepers and should take appropriate steps to keep children safe. A substantial number of children are seeing online pornography at this age, but may not yet have received education about sexuality, consent, and respectful relationships to help them critically interpret this content. Age-appropriate education could help prevent and mitigate its influence.
- Children between the ages of 13 and 15 are more likely to be using their own devices, without supervision. Children at this age are also permitted to join most social media services. It is common for children to see online pornography on social media services – both those which permit pornography and those which do not. If a service allows pornography, it should apply settings to prevent it from being accessed by and recommended to children. Among other things, this requires robust age assurance measures at sign-up to ensure the service knows the age of its users. If a service does not allow pornography, this rule needs to be enforced through effective reporting mechanisms and proactive content detection and moderation tools, developed and deployed in consultation with the user community.
- Stakeholders were least concerned about children aged between 16 and 17 accessing online pornography, as they are old enough to consent to sex and are more likely to have received education about sexuality, consent, and respectful relationships by this age. However, children at this age continue to have unintentional and unwanted encounters with online pornography. Online services should seek to minimise the potential for unintentional encounters with online pornography and give users control over their experiences and what they see.

- There is a risk that age assurance measures have the potential to deter users from accessing compliant sites. Instead, they may follow the path of least resistance toward sites which do not comply with age requirements. Accordingly, consideration should be given to complementary interventions in other parts of the digital ecosystem to prevent children from landing at high-risk sites and services in the first place, as well as preventing non-compliant sites from being surfaced at the top of search results.

Next steps and recommendations snapshot (see page 54 for full details)

eSafety:

- Raise awareness and provide practical guidance for appropriate interventions across the digital ecosystem through industry engagement, including the Safety by Design initiative.

Australian Government:

- Establish an online safety tech centre which serves to support parents, carers, and others to access, understand, and apply safety technologies that work best for their family's circumstances as one part of a holistic approach to online safety.

Activities for awareness raising and education

Key findings

- The importance of education was highlighted time and again in the research submitted to and conducted by eSafety, as well as in the consultations held across nearly all stakeholder groups – including children and young people themselves.
- Age-appropriate, inclusive, evidence-based, and stigma-free education about online pornography and the related topics of sexuality, consent, and respectful relationships should be available not only to children and young people, but also to the adults who support them to navigate these issues as they mature. This includes parents and carers, educators, and frontline workers. As set out above, parents, carers, and others also need information about technological measures they can apply.
- Education which applies a gender lens and is inclusive of all sexualities may increase resilience to sexist and violent scripts commonly found in mainstream pornography. It may also reduce the likelihood that LGBTIQ+ young people find their sexual education inadequate and seek out information from other sources such as pornography.
- There is a wealth of existing initiatives and good practice to build on in this space, and an array of new work commencing – particularly in the areas of consent, respectful relationships, and prevention of gender-based violence. Ongoing collaboration and coordination will be needed to fill gaps and avoid duplication.
- In addition to information about online pornography and complementary safety tech measures, the introduction of any age assurance pilot or regime should be supported by communication and awareness-raising initiatives to build public knowledge and trust. This should include information about what age assurance is, what measures are in place to support user privacy, and options to use alternative mechanisms if one technology provides inaccurate results or is not easy to access.

Next steps and recommendations snapshot (see page 70 for full details)

eSafety:

- Develop evidence-based, age-appropriate educational resources about online pornography with and for children and young people.
- Continue to collaborate across government to integrate resources into relevant curricula and promote best practice approaches through existing networks.

Australian Government

- Fund eSafety to develop and raise awareness of tailored resources for specific groups of children and young people, as well as complementary resources for parents and carers, educators, and frontline workers about online pornography and safety technology.
- Develop a mechanism for greater national coordination and collaboration of respectful relationships education.
- Implement awareness raising in consideration of a pilot.

Mandatory age assurance mechanism

If and how a mandatory age verification mechanism or similar for online pornography could practically be achieved in Australia

Background

While the roadmap focuses on children's access to online pornography, the ability of online service providers to ascertain the age of their users is essential to keeping children safe from a wider spectrum of risks and harms beyond pornography.[5] The development of this capability is a core example of a Safety by Design approach, whereby industry creates safe, private, engaging, and age-appropriate online experiences for the community.[6]

Consistent with stakeholder feedback and global developments, the roadmap considers the broader range of age assurance technologies (such as age estimation) rather than limiting its assessment to age verification.

Age assurance is an umbrella term which includes both age verification and age estimation solutions. The word 'assurance' refers to the varying levels of certainty different solutions offer in establishing an age or age range.[7]

Age verification measures determine a person's age to a high level of accuracy, whereas age estimation technologies provide an approximate age to allow or deny access to age-restricted online content or services. An example of age verification is the use of physical or digital government identity documents to establish a person's age.

Age estimation can involve the use of biometric data, such as a facial scan or voice recording, to infer a person's age or age range.

For the purposes of our research, consultation, and background report, we used a broad definition of online pornography: 'online material that contains sexually explicit descriptions of displays that are intended to create sexual excitement, including sexual intercourse or other sexual activity'. Starting with a broad definition allowed eSafety to consider a wide range of issues and consider research which uses varied definitions of online pornography.

The 2017 Australian Institute of Family Studies (AIFS) report notes there is no singular type of pornography – there is substantial diversity in the forms pornography can take (text, images, video, and audio) as well as the content and production context.[8] This point was also raised throughout our consultations, with stakeholders highlighting that the risks of harm to children may vary depending on the nature of the pornography and other factors.

In line with eSafety's regulatory posture and priorities and the Committee's recommendations, eSafety has taken a risks- and harms-based approach to this roadmap.[9]

Global and industry developments

Australia is not alone in exploring how age assurance can contribute to preventing and addressing online harms to children. Countries including France, Germany, and the UK are considering or implementing age assurance requirements.[10] As a result, the online industry is increasingly adopting more robust approaches to determining their users' ages beyond asking them to self-declare their date of birth. Between the Inquiry in 2019 and March 2023 several companies announced measures relating to user ages. For example:

Roblox is a game-creation platform that allows users to design their own games and play a wide variety of games created by other users. In September 2021, Roblox announced its new Chat with Voice feature, which allows players to communicate with one another, would be available for early access to all users who verify they are at least 13 years of age through an ID scan accompanied by a selfie match to ensure 'liveness' and 'likeness'.[11]

In March 2022, Google announced a new age verification step for Australian users of YouTube, a video-sharing social media service. When attempting to access age-restricted content on YouTube or downloading on Google play, some Australian users may be asked to provide additional proof of age. Google will use this additional step to assure whether a user is above 18, regardless of the age associated with the user's account. If Google is unable to substantiate that the user is over 18, that user is asked to verify their age, by providing either a photograph of a government-issued ID or by allowing an authorisation on their credit card.[12]

Yubo is a location-based social media app for teenagers to connect with other young people in their local area. In May 2022, it announced the introduction of an age verification system developed in partnership with Yoti[13] to allow users to be confident they are interacting with others of a similar age group. Yubo first launched the use of Yoti's facial age estimation technology for users aged 13-14, with the goal of scaling the technology across its entire user base by the end of the year. Yubo's announcement noted this was a first for a social media service of its size.[14]

In June 2022, Meta announced it was testing new options for users to verify their age on its photo- and video-sharing social media service, Instagram, to give them age-appropriate experiences. In addition to providing ID, new options for users included asking others to vouch for their age and taking a video selfie to be shared with Yoti for facial age estimation. In March 2023, this trial was rolled out in Australia.[15]

Despite this progress, significant gaps remain.

Public perceptions and important factors

More than three in four Australian adults surveyed as part of our public perceptions research supported the implementation of age assurance technology by the Australian Government to confirm users meet a minimum age to access online pornography.[16]

This is consistent with similar research conducted by others.[17]

However, some respondents reported low confidence in the successful design, implementation, and operationalisation of an age assurance regime, including its effectiveness and ability to safeguard privacy and security. These themes – as well as concerns about accessibility, fairness, and bias – were echoed in eSafety's research with 16-18-year-olds, conversations with the eSafety Youth Council, and broader stakeholder consultations.

Based on the key factors which emerged from our research and consultations, eSafety developed a set of criteria – comprising design and implementation factors – to assess different categories of age assurance technology.

Design factors include:

- level of assurance
- feasibility, including whether the technology is ready to be rolled out and effective in practice
- extent and sensitivity of the data required for the technology to operate
- security and technical integrity of the technology
- accessibility, barriers to inclusion (for example, if access to particular devices or forms of ID is required) and potential for bias (for example, if age estimates may be affected by skin tone, gender, or other characteristics).

Implementation factors include:

- transparency and accountability in relation to decision-making, and availability and accessibility of appeals processes
- governance and risk management processes
- flexibility to account for different business models
- certification, accreditation, or auditing against minimum standards
- compliance with privacy legislation
- trustworthiness of the technology (both perceived and actual)
- independent oversight
- availability of multiple options to enable customer choice
- fairness, accessibility, and equity
- compatibility with human rights considerations
- proportionality to the risks of harm based on the best available evidence.

eSafety commissioned Enex Testlab to carry out an independent assessment of age assurance technologies available on the market, including facial and voice age estimation tools (biometrics), as well as tools which rely on identification documents.

Findings from the independent assessment

The independent assessment found facial analysis tools, which use machine learning models to estimate a person's age based on their facial proportions and characteristics (and which then delete the image), to be the most viable and privacy-preserving within the biometrics category.[18] This is despite concerns these technologies may create barriers to inclusion as they may not perform well for some skin tones, genders, or those with physical differences. In consultations, stakeholders also raised concerns in relation to the collection and use of sensitive biometric information.[19]

Voice age analysis and capacity assessment tools are less mature. The independent assessment also pointed out voice analysis and capacity testing tend to be limited by the fact a person's ability to read, speak, or write does not always correlate to their biological age. In addition, they can be affected by accents, low language fluency or disability, also potentially creating barriers to inclusion.

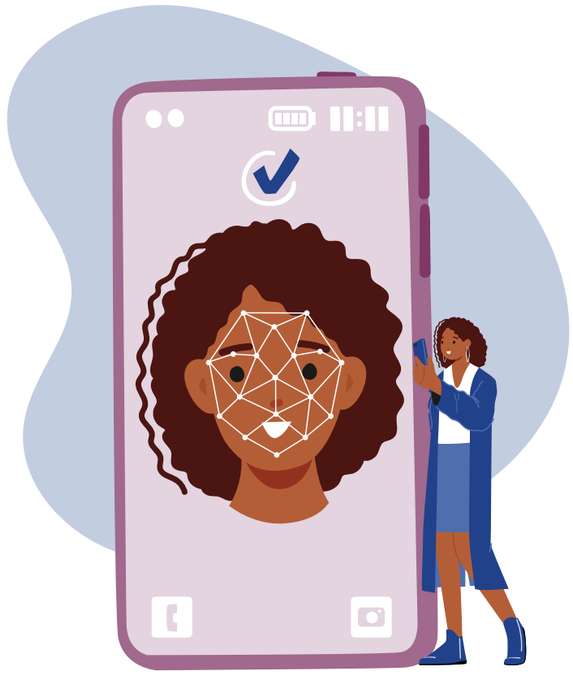
Enex Testlab tested two solutions which use hard identifiers to verify a person's identity, including their age.[20] The identifying information is stored securely on their mobile device and is capable of being reused when needed. As with other products which require government-issued documents for identity verification, this can create barriers for those who do not have access to such documents. However, the use of such identifiers is common and offers a relatively high level of age assurance compared to other options. While there are risks in relation to privacy and security, the use of trusted and accredited third-party providers with strong privacy and security practices may mitigate these risks.[21]

The independent assessment also reviewed the status of relevant international standards and findings from recent age assurance trials conducted by euCONSENT in Europe.[22]

Given potential concerns with privacy and security, one of the most relevant components of the euCONSENT pilot was the use of a 'tokenised', interoperable, and double-blind approach to preserve user anonymity. This is where age-restricted websites do not know the identity of a user, and the age assurance service provider does not record which sites a user visits.

An electronic token can be produced once a person's age is verified or estimated by an age assurance provider.[23] Rather than providing a user's specific age, tokens can be limited to confirm whether a user meets a minimum age requirement. This allows the online service to confirm age requirements are met without viewing or collecting users' personal information. The system can be designed so the token is stored in a device's digital wallet or browser and may be reused for a period of time, when trying to access age-restricted services requiring the same level of assurance. This can serve to reduce friction for users and to reduce regulatory burden for age-restricted services. Implementation of this mechanism can be tailored to the relevant age-restricted service and parameters of the system.

French data regulator, Commission Nationale Informatique & Libertés (CNIL), in partnership with cryptography researchers, has also developed and released an open-source demonstration of a zero-knowledge proof exchange based on cryptography concepts.[24] Models like this allow only the age attribute to be shared and shares neither information about the user's identity with the age-restricted service nor information about the nature of the age-restricted service with the provider of the age attribute. This may mitigate concerns about user privacy, and in particular concerns about tracking users' online behaviour.



The independent assessment's main finding is the age assurance industry and its associated technologies are new and still evolving. The assessment suggests age assurance technologies should be trialled in the Australian context before being prescribed, building on lessons learned through the euCONSENT pilot. In particular, Enex Testlab supported the development of an internationally defined age token and the provision of multiple accredited options for consumers to select their preference for proving their age. They noted the benefits of storing such tokens at the device level through digital wallets and suggested any age assurance regime should be aligned with existing and developing Australian frameworks discussed below in 'legislative and regulatory framework'.

Age assurance requirements and expectations under existing regulations

The *Online Safety Act 2021* (Cth) includes an Online Content Scheme providing eSafety with powers to regulate and, in some cases, remove illegal and restricted content, defined by reference to the National Classification Scheme.[25] Pornography may be class 1 (Refused Classification) or class 2 (X18+ or R18+) content, depending on its nature.

- **Class 1 (RC) online pornography:** This includes material that depicts, expresses, or otherwise deals with matters of sex, cruelty, or violence in a way that offends against the standards of morality, decency, and propriety generally accepted by reasonable adults. Under the *Guidelines for the Classification of Films 2012*, this covers depictions of sexual or sexualised violence, sexually assaultive language, and consensual depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers. It also covers specific fetish practices, including body piercing, application of substances such as candle wax, 'golden showers', bondage, spanking, or fisting.
- **Class 2 (X18+) online pornography:** Other sexually explicit material that depicts actual (not simulated) sex between consenting adults.
- **Class 2 (R18+) online pornography:** Material which includes realistically simulated sexual activity between adults, or high-impact nudity or violence.

eSafety's powers in relation to such content differ depending on the classification or likely classification. In some cases, eSafety can issue enforceable removal notices and in other cases, eSafety can issue enforceable remedial notices requiring class 2 material to be placed behind a restricted access system (**RAS**).[26] The operation and limits of the RAS provisions are described in more detail in the legislative and regulatory framework section below.

The Basic Online Safety Expectations (**the Expectations**)[27] and the industry codes or standards are also described in detail below. Expectations include that social media services,[28] relevant electronic services,[29] and designated internet services[30] take reasonable steps to prevent access by children to class 2 material, which includes pornography. The industry codes or standards under the Act are being developed in phases. The first phase, focusing on child sexual exploitation material and material that is pro-terror or contains extreme crime and violence, is currently in progress.[31] Following its completion, the second phase will commence. This will focus on children's access to high impact material, including pornography.

Evidence to inform such a mandate

In considering if and how age assurance mechanisms for online pornography could be mandated through these or other avenues to prevent and mitigate harm to children, it was important to review the research on the nature of children's encounters with online pornography and associated risks and impacts.

However, there are limits to the research and literature, and it can be difficult to disentangle the potential impacts of online pornography from the broader context in which it is situated.[32]

To ensure this report was informed by the experiences and views of children and young people, eSafety conducted primary quantitative and qualitative research with participants aged 16-18. This research explored participants' lived experience in relation to their encounters with, and ideas about, online pornography; the support they want to receive about navigating online pornography; and their views on age-based restrictions of online pornography and age assurance technologies.

There are a wide range of individualised factors for children which may affect their experiences with online pornography, and their risk or experiences of harm – including age, gender, education, relationship with parents or carers, other experiences of abuse or harm, their family, and cultural views on pornography.[33] We heard a diverse range of views and experiences from both our stakeholders and our research participants aged 16-18.

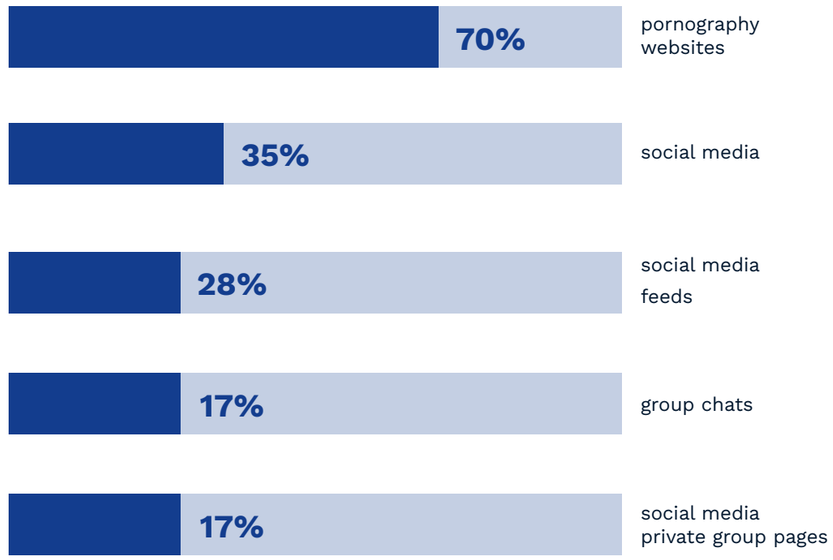
Many children encounter online pornography unintentionally,[34] as discussed in the 'complementary measures' section below. When children seek out pornography, they do so for curiosity and for sexual arousal but also boredom, relaxation, education, and as a joke. While most pornography may not provide sound advice about consent and safer sex practices, a systematic review published in 2020 found pornography can offer viewers, especially gay male viewers, useful information about the mechanics of sex, as well as allowing viewers to explore and learn about their own sexual identity, sexual desire, and sexual pleasure.[35]

In our research, LGB+[36] participants were also significantly more likely to say there were some positive effects of online pornography on young people learning about sex and exploring their sexuality than straight participants. Some stakeholders reflected this may be due to a lack of other representations or learning sources for young LGBTIQ+ people – including a lack of inclusive sex education in schools.[37]

Most research participants aged 16-18 thought there were negative (negative or very negative) effects of online pornography on young people's understanding and expectations of consent (74%), sex (76%), relationships (76%), and gender (64%).[38] A smaller proportion of the young people surveyed (43%) thought online pornography had a negative or very negative effect on young people learning about sex and exploring their sexuality.

Research submitted to and conducted by eSafety shows it is common for children to see online pornography.[39] There is significant variation in when, where, and how they see this content, as well as in the type and form of content they find. For example, findings from eSafety's research with 16-18-year-olds revealed almost half (47%) the participants who had seen online pornography first encountered it when they were 13, 14, or 15 years old. Places where they encountered this content varied from pornography websites (70%), social media feeds (35%), ads on social media (28%), social media messages (22%), group chats (17%), and social media private group/pages (17%). Younger participants were more likely to report unintentional encounters with online pornography compared to 18-year-olds (74% v 60%) while 18-year-olds were more likely to report intentional access (69% v 51%).

% of 16-18-year-olds who had seen online pornography first encountered it when they were 13, 14, or 15 years old



Places where they encountered this content

Our research found that several demographic factors, including non-heterosexual identity, impacted on the age when the young people surveyed first encountered online pornography. LGB+ young people (54%), young people with disability (53%), and/or young people who speak a language other than English at home (LOE; 47%) were significantly more likely to first encounter online pornography before the age of 13 compared to the general sample (39%).

While the research is complex, and in some cases, conflicting, the main harm which emerges is an association between **mainstream pornography** and attitudes and behaviours which can contribute to gender-based violence.[40] Other potential impacts and harms, including connections between online pornography and harmful sexual behaviours, and risky or unsafe sexual behaviours, are explored at length in eSafety's background report. This report adopts the definition of mainstream pornography developed by the Australian Institute of Family Studies (AIFS): predominately video content, targeting a male heterosexual audience, and forming a significant proportion of the global pornography market.[41] Some studies have characterised the nature of mainstream pornography as containing and normalising depictions of sexual violence and degrading sexual scripts about women.[42]

eSafety consulted both large, international providers of online pornography, as well as local industry bodies representing Australian sex workers and pornography producers and performers. This consultation highlighted significant differences within the industry.

Local industry bodies submitted that many producers of content domestically are female and/or LGBTIQ+ and operate as sole trader producer-performers.[43]

In comparison, MindGeek, a Canadian company, employs more than 1,800 people worldwide[44] and owns one of the most popular pornography video aggregator sites (Pornhub), several other aggregator sites and multiple major production brands such as Brazzers and Reality Kings.[45] This has resulted in significant centralisation of ownership over both content production and distribution. MindGeek's website states the company gets 115M+ daily visitors across their web properties, serving 3 billion+ advertising impressions.[46]

Between these two ends of the spectrum are a variety of businesses with different business models and levels of size, maturity, capacity, and capability to adopt technological measures to promote children's safety. What constitutes appropriate steps for one provider might create an undue burden for another. In determining what is proportionate and reasonable in the circumstances, it is important to consider the potential differential in risk to children posed by different types of services.

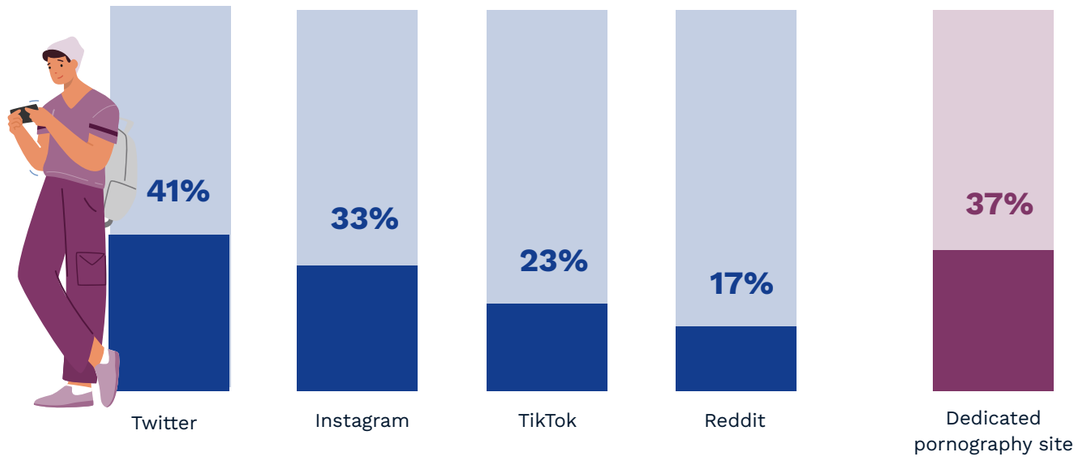
Some of the most accessed pornography sites from Australia, in order of popularity,[47] are Pornhub (owned by MindGeek S.A.R.L based out of Luxembourg and Canada, and recently acquired by Ethical Capital Partners), Xvideos and Xnxx (both owned by WGCZ Holdings and based in the Czech Republic), XHamster (owned by Hammy Media based in Cyprus), and Chaturbate (owned by Triplebyte and based in the US).

Given the reach of these large businesses – and the nature of the content freely available on their homepages – they have a particularly significant responsibility to take reasonable steps to prevent children from accessing their services. A 2021 study in the UK analysed the titles of more than 130,000 videos from Pornhub, XHamster, and XVideos and found 12% of videos shown to first-time users on a homepage described sexual activity that constitutes sexual violence.[48]

As of November 2022, Pornhub was the most popular pornography site in Australia and the 14th most visited website from Australia overall.[49] On average, there are 13,600,000 monthly Google searches for 'pornhub' from Australia.[50] Pornhub is also one of the most popular sites worldwide, with an estimated 33 million European Union (EU) monthly users[51] and 2.3 billion monthly total visits worldwide.[52]

Many of these services are also subject to legal enforcement action from regulators who have implemented requirements of age verification. While these sites are often tagged as 'Restricted to Adults', and XHamster has an age gate for first time visitors, their services have little else in place to prevent children from accessing this content. France and Germany have taken regulatory action against Pornhub and Xhamster for allegedly failing to restrict children's access to pornography.[53] France has also taken regulatory action against Xvideos and Xnxx.[54] These enforcement actions are ongoing – international regulators have faced challenges enforcing national law on international companies and with non-compliant sites using 'mirror' sites to circumvent blocking orders.

Online pornography is also found on a range of other sites and services. A recent survey commissioned by the Children's Commissioner in England found 41% of participants (16-21) who had seen online pornography had viewed it on Twitter, a social media service which allows pornography but requires it to be tagged as sensitive and hidden from under 18 accounts.[55] This was more than dedicated pornography sites (37%) and other social media sites (Instagram 33%, TikTok 23%, Reddit 17%).[56]



Social media services where 16-18 year olds have seen pornography

[UK Children's Commissioner, 'A lot of it is actually just abuse': Young People and Pornography, January 2023]

A mandatory age assurance mechanism, on its own, will not address the issue of pornography's influence and association with attitudes and behaviours which can contribute to gender-based violence.[57] However, to the extent age assurance and other forms of safety technology may increase the age at which children are likely to encounter online pornography featuring sexism, misogyny, or gender-based violence, they may also contribute to reducing harmful attitudes and behaviours towards girls and women. This provides opportunities for children to receive respectful relationships education prior to viewing such content. As discussed below in 'education', starting online safety and respectful relationships education early, and reinforcing it often to support critical thinking skills and provide counter-narratives to harmful scripts often present in mainstream pornography is crucial.

Coordination with the National Plan

The relationship between pornography and violence is also an important component of the broader National Plan to End Violence against Women and Children 2022-2032 (**National Plan**), which outlines what needs to happen to achieve the vision of ending violence in one generation. The National Plan gives specific attention to pornography and explicitly names it as a key area of focus for addressing gender-based violence in Australia. Accordingly, it will be important to coordinate any initiatives flowing from this report with the Department of Social Services and others implementing violence prevention efforts under the National Plan.

Remaining gaps in evidence

There are still substantial gaps in the evidence base. These include the experiences of First Nations children. While we know from eSafety's recent research that the prevalence of access is similar among First Nations children, we do not have a clear understanding of how their experiences and support needs may differ. Representatives from eSafety travelled to several regional and remote First Nations communities across the latter half of 2022 and spoke to several Aboriginal community members aged 10-70 about a range of online safety issues. In the majority of these discussions, community members raised, without prompting, the topic of children's access to online pornography and their perceptions and concerns of its impact on the child and their community at large.

Research is also needed on the experiences of younger children, and those who are culturally and linguistically diverse. In addition, research on the intersections between online pornography, harmful sexual attitudes and behaviours, and emerging technologies such as generative artificial intelligence[58] and immersive environments[59] is limited due to the nascence of these technologies. There will be an ongoing need for research as the nature of the online environment and the risks to children continue to evolve.

While further research is needed, the available evidence provides sufficient direction for initial action.

Roadmap

eSafety's proposed next steps

1. Coordination

- eSafety will continue to work with the Department of Social Services(DSS) and others to progress the National Plan, particularly those activities relating to mainstream online pornography as a contributor to harmful gender stereotypes.

2. Research

- eSafety will publish the research we conducted with 16-18-year-olds about their experiences with and attitudes to online pornography, as well as their views about age verification. This will contribute to the available evidence base.

Recommendations for the Australian Government

1. Fund specialist researchers and experts in working with younger children on sensitive issues to conduct research examining:

- The content of online pornography that children and young people are encountering.
- The impacts on and feelings of children and young people.
- What children and young people are learning from online pornography.
- Pathways into and factors that influence encounters with online pornography.
- How emerging technologies and online environments, such as virtual/augmented/extended reality and the metaverse, change the ability to access and the nature of engagement with online pornography, and the potential impacts on children.
- Attitudes towards and impacts of online pornography among at risk groups, especially those who are underrepresented in current research, including Aboriginal and Torres Strait Islander and culturally and linguistically diverse children and young people.
- The experiences and impacts of online pornography on children and young people under 16, and especially under 12.

2. Develop, implement, and evaluate a pilot before seeking to prescribe and mandate age assurance technologies for access to online pornography.

- eSafety recommends a trial of age assurance technologies and the use of digital tokens in the Australian context. This reflects international experience, similar state initiatives such as Service NSW's digital age verification pilot and aligns with independent technical advice.
- While eSafety should be involved in the development, implementation, and evaluation of any such pilot, we do not presently have the resources or expertise to lead its delivery.
- eSafety recommends the Australian Government consider the following arrangements in relation to a pilot. These are in addition to the considerations relating to cross-government stewardship raised below in the 'legislative and regulatory framework' section:

Privacy impact assessment: *The Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) requires Australian Government agencies subject to the *Privacy Act 1988* (Cth) to conduct a privacy impact assessment for all high privacy risk projects.

Collaboration with euCONSENT: Consistent with our independent technical advice, and to facilitate international harmonisation and build on lessons learned to date, eSafety recommends working with the euCONSENT consortium and building on the outcomes of their European trial of an interoperable, privacy-preserving, and choice-enhancing age assurance system.

Multiple use cases: As in the euCONSENT project, eSafety recommends the initial trial be conducted using dummy sites with different use-cases. In addition to online pornography, these could include online wagering and online alcohol sales, though we note there are already several initiatives underway in these areas.[60] Alternative use cases could include establishing minimum age to use a social media service, and/or determining age for purposes of providing consent to collection of personal information. If the pilot is successful, and government decides to implement an age assurance mechanism, consider doing so in a way that is consistent across various age-restricted industries to reduce the risk of stigma associated with a pornography-specific measure and enable government to determine the appropriate level of assurance for each use case. Testing this technology across use cases also aligns with the findings in the myGov audit, which calls for a nationally consistent approach to digital services across levels of government.

User choice: Consistent with stakeholder and technical feedback, eSafety recommends the pilot provide users with a range of options to confirm their age, including technologies that verify and estimate age. This is to be inclusive of users who do not have access to or feel uncomfortable about a particular method of age assurance.

Technologies: To promote international harmonisation, eSafety suggests technologies which have been approved for use in other jurisdictions, accredited under existing international standards, and already in use by the online industry should be prioritised for inclusion in a pilot.

Double-blind, tokenised approach: Due to stakeholder support for, and an increasing international adoption of, the privacy-preserving tokenised double-blind approach to age assurance, eSafety recommends this Australian pilot is designed to test this approach and its reusability through digital wallets. eSafety additionally recommends its trial using a device-based token as opposed to one stored in a browser to aide user experience. The pilot could utilise a third-party exchange provider to transfer information with consent between dummy sites and age assurance providers to further protect user privacy. Compatibility with the Trusted Digital Identity Framework and complementary government processes would be beneficial should government choose to support an ongoing system beyond the pilot, to reduce the regulatory burden on commercial providers who participate in both age assurance and identity verification.

Consultation: eSafety recommends ongoing input from the stakeholder groups consulted for the development of this report, including children and young people, parents and carers, the adult industry, the online industry, digital rights advocacy groups, and academics, researchers, and non-government organisations (NGOs) across a range of relevant disciplines.

Awareness raising: Following findings from eSafety's research, eSafety recommends the pilot be accompanied by a campaign to educate and increase public awareness of how these technologies work, including how they use, store, and protect data.

Comprehensive and transparent evaluation: eSafety suggests the pilot be evaluated against a pre-established set of criteria, which could include accuracy and effectiveness of technology, barriers to inclusion and digital participation, bias, user experience, compatibility with human rights, extent of interoperability, and whether participants have the option to exercise granular control over their privacy and are provided with resources to support their informed consent to sharing data. Note this is not an exhaustive list but an indication of the breadth of considerations in delivering a successful pilot.

Cross-government stewardship: As explained in the next section, eSafety believes any the pilot should be a cross-government initiative with engagement from multiple agencies and departments working on issues at the cross-section of online safety, privacy, security, and human and consumer rights.

Legislative and regulatory framework

A suitable legislative and regulatory framework

The Committee recommended that the roadmap consider a suitable legislative and regulatory framework for implementing mandatory age assurance. eSafety suggests there are two parts to this legislative and regulatory framework.

Online safety regulatory framework

The first part would establish the expectations and requirements for service providers within the online industry to apply age assurance and other complementary measures to prevent, or limit, children's access to online pornography.

Online Safety Act

The Online Safety Act 2021 (Cth) can help fulfill this component, as the existing Australian framework for promoting online safety and seeking to regulate online access to such content. The Act, which took effect in January 2022, covers many of the key sections of the online ecosystem. In addition to social media services, relevant electronic services and designated internet services defined above, there are provisions which apply to hosting services,[61] app distribution services,[62] search engine services, internet service providers[63] and those who manufacture, supply, maintain or install certain equipment.[64] The Minister is to initiate an independent review of the Act by January 2025,[65] providing an important opportunity to consider potential issues for reform identified in this paper. The review of the Act and any subsequent reforms are also likely to be informed by consultation and accompanied by awareness raising efforts.

Classification, removal, and remedial powers

The Act's Online Content Scheme defines material by reference to the National Classification Scheme. Pornography is not a distinct category of material under the Scheme – instead, online pornography is classified as Refused Classification (RC), X18+ or R18+, depending on what it contains.[66] eSafety's powers under the Act differ depending on the actual or likely classification.

If material is or is likely to be classified RC (i.e., class 1 material), eSafety can issue enforceable removal notices, regardless of where it is hosted or provided from. If material is X18+ or is likely to be X18+ (which the Act treats as a subset of class 2 material), eSafety can issue enforceable removal notices, but only if it is provided from Australia. If material is likely to be R18+ (which the Act treats as a different subset of class 2 material) and is provided from Australia, eSafety can issue enforceable remedial notices requiring it to be placed behind a restricted access system (RAS).[67]

A RAS is an access-control system that meets the requirements set out in the *Online Safety (Restricted Access Systems) Declaration 2022* (Cth) (**RAS Declaration**). Rather than specify or prescribe technologies or processes to be used by service providers, the RAS Declaration states an access-control system must:

- require an application be made by a person in order to access the relevant material, declaring they are at least 18
- incorporate reasonable steps to confirm an applicant is at least 18
- give warnings about the nature of the material and safety information about how a parent or guardian may control access to the material and
- limit access to the material unless certain steps are followed.

During eSafety's consultations, some stakeholders said the current regulatory framework for online pornography, and its reliance on the National Classification Scheme, is outdated and problematic. They pointed to the current prohibition on specific categories of consensual fetish content,[68] and its potential to stigmatise and censor queer sex practices and content, as an example. In addition, with online pornography potentially falling within three separate classification categories depending on the precise nature of the content, some stakeholders felt there was scope for confusion among regulated entities.

Some stakeholders also highlighted the inconsistency between the age to access pornography (18) and the age of consent to sex (generally 16 or 17 depending on the state or territory).[69] They felt the age of consent could be used to guide the age of access to online pornography. This was echoed in our focus groups with 16-18-year-olds, and eSafety's survey of 16-18-year-olds which found one in two respondents think the age of consent should factor into the age to access to online pornography. The current age differential may create particular challenges in immersive environments, where the lines between pornography as online content versus pornography as sexual activity may be blurred.

The context in which the National Classification Code and classification guidelines were created is very different to the modern online environment. There is now a far greater diversity and volume of content, as well as a greater capacity for users to view content and create and distribute content themselves.

On 16 December 2019, the then Minister for Communications, Cyber Safety and the Arts released terms of reference for a review of Australia's classification regulation.[70] This review sought to develop a classification framework that meets community needs and reflects today's digital environment. The review (the Stevens Review) was published on 29 March 2023.

Any outcomes from the review or future reform of the classification regulation, and their potential implications for the Online Content Scheme, will need to be considered through the review of the Act. eSafety will continue working with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), the department which has policy responsibility for classification and online safety.

In addition to these removal and remedial powers, which serve as a safety net to address individual items of content, the Act provides for broader regulatory schemes. These include the development of industry codes or industry standards.

Industry codes and standards and service provider determinations

The Act provides for industry bodies to develop industry codes to regulate certain types of harmful online content, and for eSafety to register an industry code if it meets certain statutory requirements, including the provision of appropriate community safeguards.[71] Industry codes are to cover eight key sections of the online industry across the digital ecosystem, including social media, messaging services, search engines, app distribution services, designated internet services (including many pornography sites), suppliers of equipment used to access online services and internet service providers. If eSafety finds a proposed industry code does not meet the statutory requirements, eSafety can determine an industry standard setting the measures for the relevant section of the online industry. Both industry codes and industry standards are enforceable through various mechanisms including injunctions and civil penalty proceedings.

eSafety has been liaising closely with industry in relation to the first phase of industry codes which seek to regulate the availability of class 1 material including child sexual exploitation material, pro-terror and extreme crime and violence.

On 9 February 2023, the eSafety Commissioner wrote to the industry associations to inform them of her preliminary views that the first phase of industry codes, submitted in late 2022, do not provide appropriate community safeguards and are unlikely to meet the statutory requirements for registration. The eSafety Commissioner invited the industry associations to respond and/or resubmit draft industry codes that address eSafety's feedback. Revised industry codes are due to be provided to eSafety by 31 March 2023.

The development of the second phase of industry codes, which will commence once phase 1 industry codes or industry standards are in place, will seek to address children's access to high impact content and forms of online pornography (whether likely to be RC, X18+, or R18+), informed by this report. Accordingly, the second phase of industry codes or standards will be an important avenue to require regulated entities to implement some of the good practices for age assurance and complementary measures identified in this report.

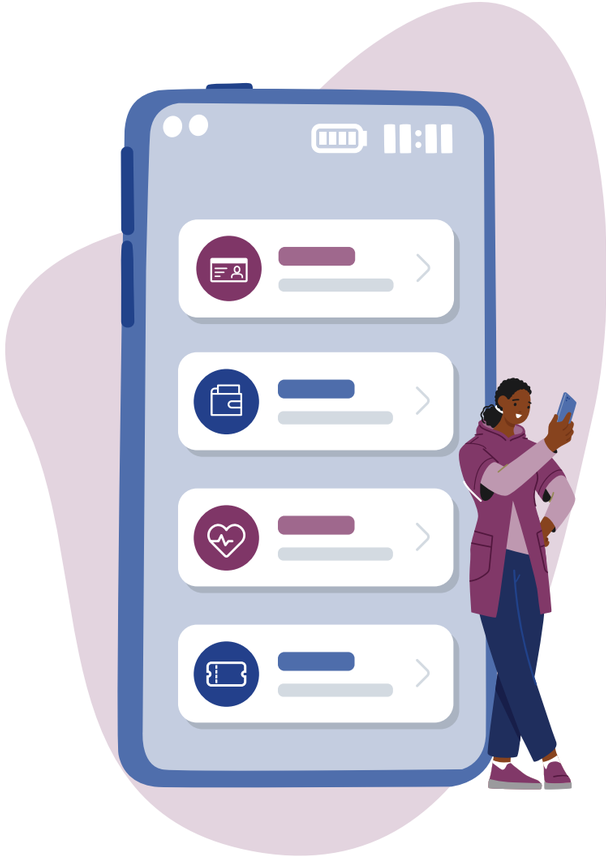
In addition to industry codes and standards, the Act's Online Content Scheme also enables eSafety to develop Service Provider Determinations setting out enforceable rules about matters where the Minister has previously specified legislative rules for such matters.[72] It is a matter for the Minister whether service provider determinations could be made in relation to online pornography, considering the ongoing processes in relation to industry codes and/or industry standards. Notably, Service Provider Determinations could apply to most but not all the sections of the online industry covered through industry codes or industry standards.[73]

Basic Online Safety Expectations

The Act also provides for the Minister to set online safety expectations for service providers called the Basic Online Safety Expectations (the Expectations).[74] The Expectations,[75] determined in January 2022 by the then-Minister, set out, among other things, that providers should take reasonable steps to make sure technological or other measures are in effect to prevent access by children to class 2 (X18+ or R18+) material.[76] They apply to three of the eight sections of the online industry which are covered by industry codes or standards.[77] The reasonable steps to meet the Expectations will differ by service, depending on the user base, functionality, and policies. For some Expectations, the Determination sets out examples of reasonable steps that could – but are not necessarily required – to be taken.[78]

Unlike the commitments to be contained in registered industry codes or determined by industry standards, compliance with the Expectations is not enforceable. However, eSafety may exercise powers under the Act to require providers to report on the steps they are taking to meet the Expectations. There are financial penalties for providers that do not respond to a reporting requirement. In addition, eSafety can publish a statement that a provider has or has not complied with relevant Expectations. This improves transparency and accountability and introduces an element of reputational risk for non-compliance.

Providers should have started reviewing their systems, processes, and policies to ensure compliance when the Expectations commenced in January 2022. Importantly, service providers are expected to take reasonable steps to comply with the Expectations now, rather than waiting for outcomes of any government pilot.



Upon release of this roadmap, service providers can and should consider the good practice measures identified in determining what steps may be reasonable to take.

eSafety has also committed to giving further guidance where necessary to support providers in determining the reasonable steps to implement the Expectations.[79] Such guidance will be informed by this roadmap and the background report.

In addition, information obtained from responses to reporting notices will continue to inform eSafety's approach to these issues, and understanding of measures industry can take, as well as informing any potential age assurance pilot or mandate.

Compliance and enforcement

eSafety has a range of compliance and enforcement powers under the Online Content Scheme. These include warnings, infringement notices, enforceable undertakings, and court-ordered injunctions or civil penalties.

In some cases, where services have failed to comply with removal notices in relation to material likely to be RC, eSafety can issue link deletion notices to search engines or an app removal notice to an app store to prevent them from facilitating access to the material. Removal or remedial notices can also be issued to hosting services in some cases.

In circumstances involving multiple violations of civil penalty provisions which have caused the continued operation of an online service to represent a significant community safety risk, eSafety can seek a Federal Court order to stop the provision of the service.

In countries such as France and Germany where legislation requiring age assurance is already in place, enforcement has proven challenging, and court processes – including court-ordered mediation – have continued, in some cases, for several years. This points to the benefits of the regulator being empowered to issue notices to other entities within the online ecosystem who can take immediate action to prevent and mitigate harm emanating from a non-compliant service. For example, when the operation of the Act is being reviewed, consideration could also be given to the appropriateness of an additional ISP blocking power (beyond the current, time-limited power in relation to abhorrent violent conduct-related material) for circumstances where services are providing children with access to online pornography, and other measures have proven ineffective to mitigate these risks. The experience of other jurisdictions points to the need for such notices to apply to 'mirror' sites. These are duplicate sites created to circumvent regulatory or legal enforcement action, including to bypass ISP blocking orders for failure to comply with age assurance requirements.

There may potentially be a role for third parties that perform a critical role in supporting websites – such as domain administrators, registrars, or payment providers – to help prevent recidivism and increase compliance. eSafety is continuing to consider the nature of such a role, taking into account a range of factors. eSafety's views on the role that could be performed by such parties, and any associated legal powers to be conferred on eSafety, will be developed further prior to the upcoming review of the Act. The review could also consider the adequacy of the Act in relation to online harms on emerging technologies such as immersive technologies, decentralised services, and generative AI.

Privacy, security and governance regulatory framework

The second part of the legislative and regulatory framework would establish a regulatory scheme for the accreditation and oversight of age assurance providers. Before the use of specific age assurance technologies is prescribed, stakeholders told us measures need to be in place to alleviate concerns about privacy and security, and also satisfy the implementation factors raised above. These include the need for independent oversight, strong governance, transparency, trustworthiness, fairness, and respect for human rights. To promote international harmonisation, this work should be aligned with relevant international standards which are in place or under development.

There is substantial work already well underway to develop such a framework for Australia's Digital Identity System. The Australian Government should build on this work to establish a similar regulatory accreditation regime to the Trusted Digital Identity Framework for age assurance.

Establishment of such a regulatory scheme should include consideration of a strong, independent regulator or accreditation body with functions including:

- accreditation
- compliance and enforcement related to accreditation
  - enabling capabilities, such as:
  - register of accredited providers
  - application portals for prospective providers
  - any enabling IT infrastructure for the regulatory regime
- general regulatory functions – reporting, publication of guidance etc.

Based on our consultation across government, at this stage, there is likely no existing regulator or accreditation body that has the full breadth of experience and capability to provide all the necessary functions, particularly in relation to this type of digital accreditation. However, building on the work of equivalent accreditation regimes in government such as the Trusted Digital Identity Framework could provide a good basis for starting discovery work on how an accreditation scheme could operate.

The Digital Transformation Agency (DTA) is responsible for strategic and policy leadership on whole-of-government and shared information and communications technology investments and digital service delivery. Accordingly, it is an essential stakeholder in any pilot or mandate involving age assurance. In addition to the work of the DTA, there are several other important components of the overall age and identity verification landscape in Australia. This includes the recent independent review of myGov[80], the Privacy Act Review report, various initiatives and collaborations across states and territories,[81] and the Data and Digital Ministers Meeting. As the agency which designs and develops service delivery systems to meet the diverse needs of the community, in partnership with public, private, and NGO sectors. Services Australia is another critical stakeholder in this space.

The Trusted Digital Identity Framework provides that entities accredited under it must abide by the *Privacy Act 1988* (Cth) (**Privacy Act**), or a state or territory law providing an equivalent level of protection.[82] Accordingly, accredited providers will be subject to privacy obligations (either the existing privacy laws they are covered by, or by being brought into coverage under the Privacy Act). This means important privacy protections, such as the obligation to notify of a relevant data breach, will be extended to all providers.

The Privacy Act Review Report proposes that privacy impact assessments should be conducted by all entities covered by the Privacy Act prior to commencing a high privacy risk activity and that further consideration should be given to how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted.[83] It also proposes a new requirement that the handling of personal information must be fair and reasonable,[84] and a Children's Online Privacy code governing how digital platforms use children's data be introduced.[85]

A Children's Online Privacy code would clarify the principles-based requirements of the Privacy Act in more prescriptive terms and would provide guidance on how the best interests of the child should be upheld in the design of online services. For example:

- assessing a child's capacity and establishing their age
- limiting certain collections, uses and disclosures of children's personal information
- default privacy settings
- enabling children to exercise privacy rights
- balancing parental controls with a child's right to autonomy and privacy.

It is expected the code developer would be required to consult broadly with children, parents, child development and welfare experts and industry, as well as eSafety. Public feedback on the report will inform the Australian Government's next steps.

The outcomes of the Privacy Act review will have implications for age assurance and other safety measures to prevent harm to children from online pornography. Accordingly, the Attorney-General's Department (AGD) is an important stakeholder, as well as the Office of the Australian Information Commissioner (OAIC) who regulates the Privacy Act.

Clearly, there is a complex and evolving enabling environment to consider. Beyond the above components, there are also several relevant strategies, inquiries, plans and legislative proposals in relation to security, human rights, and competition and consumer rights – some of which have a particular focus on biometric technologies (such as those which conduct facial age estimation).[86] eSafety suggests the various agencies and departments involved in these initiatives should be consulted as part of any age assurance pilot or mandate. This includes the Australian Cyber Security Centre (ACSC), the Australian Competition and Consumer Commission (ACCC), the Australian Human Rights Commission (AHRC), and the Department of Home Affairs (DHA).

As mentioned above, independent technical advice suggested age assurance technologies should be trialled in the Australian context before being prescribed, building on lessons learned through the euCONSENT pilot. We accept this recommendation. Should the government support eSafety's recommendation to carry out a pilot, we suggest this should be a cross-government initiative, with input from the wide variety of government (and non-government) entities with intersecting equities, remits, and workstreams. Further considerations for a pilot are set out below.

If the Australian Government determines an age assurance system should be established and mandated following an evaluation of the pilot, eSafety suggests this will need to be supported by an appropriate accreditation framework for age assurance providers to be assessed against, and related reforms such as those relating to the Privacy Act. However, eSafety is not suggesting that Australian Government digital identity should be used to confirm age before accessing online pornography. Rather, we are suggesting that any prescribed age assurance technologies should be subject to accreditation and oversight equivalent in rigour and integrity to that of the Trusted Digital Identity Framework.

Roadmap

eSafety's proposed next steps

3. Basic Online Safety Expectations

- eSafety will continue raising awareness of the Expectations among relevant online service providers and encouraging compliance.
- eSafety will ensure guidance produced to support providers in determining the reasonable steps to implement Expectations relating to measures to prevent children's access to online pornography – including age assurance and complementary measures – is informed by the roadmap and background report.
- eSafety will continue issuing reporting notices to online service providers to enhance their transparency and accountability. Information acquired from reporting notices will continue to inform eSafety's approach to these issues and understanding of measures that industry can take, as well as informing any potential age assurance pilot or mandate.
- eSafety will provide advice to DITRDCA and the Minister in relation to how the Expectations and related provisions in the Act could be strengthened.

4. Industry codes or standards

- Development of the second phase of industry codes or standards which will address children's access to online pornography and other high impact content is expected to commence after the first phase of industry codes and/or industry standards are in place.
- The good practices, gaps, and connections identified in this roadmap and its background paper across different sections of the online industry will help inform the development of these codes, including the complementary measures set out below.

5. Coordination

- eSafety will continue to collaborate across government on intersecting initiatives and reforms, such as the classification review, the Privacy Act Review, and digital identity developments.

Factors that could be considered as part of the forthcoming independent review of the Online Safety Act

1. Any relevant outcomes from the classification review or future classification reform, with a view to applying a consistent approach to online pornography.
   - For example, consideration could be given to having a single category for online pornography, with relevant powers focused on age restriction rather than removal. Consideration could also be given to the role of a harms-based approach for some categories, instead of an approach centred on offensiveness.
2. The potential to extend various provisions of the Act to additional industry sections or entities within the digital ecosystem for the purposes of preventing children's access to online pornography and promoting compliance with the Act.
   - For example, consideration could be given to:
     - extending the application of the RAS Determination and remedial notices to services provided outside of Australia, and to content beyond R18+ material
     - extending the application of the Expectations and the service provider determinations to all the industry sections which can be covered by industry codes or standards
     - extending the application of the industry codes or standards to hosting services which host material outside of Australia
     - extending the application of ISP blocking powers to request blocking of sites (including mirror sites) which repeatedly fail to comply with requirements to prevent children from encountering online pornography
     - extending the application of the Act to notify non-compliant services to relevant domain administrators and registrars, payment providers, advertisers, shareholders, investors, and others who may cease providing support.
3. The applicability of the Act and the suitability of existing regulatory powers to address children's access to online pornography through emerging technologies, such as generative AI and immersive technologies.
4. Resourcing for the implementation and enforcement of the second phase of industry codes or standards, and the expansion of Basic Online Safety Expectations reporting notices.

Additional factors to consider for an age assurance pilot

5. In addition to the factors set out above, eSafety recommends the Australian Government consider the following arrangements in relation to a pilot:
   - Cross-government stewardship: A cross-government steering committee or consultation process should be formed to determine the best agency to progress a pilot. We suggest this could include the DTA for digital investment oversight; Services Australia for operational and implementation-related advice; ACSC, AGD, OAIC, and DHA for privacy- and security-related considerations, and AHRC on children's best interests and broader human rights considerations. In addition, we suggest ACCC could provide competition and consumer rights-related advice, DSS could contribute its expertise in the National Plan and customer verification for purposes of online wagering, and DITRDCA and eSafety could provide advice from an online safety perspective. Consultation with the Data and Digital Ministers could also prove beneficial.

Complementary measures and a holistic approach

Recommendations for complementary measures to ensure age verification is part of a broader, holistic approach to address risks and harms associated with children's encounters with online pornography

Background

In eSafety's consultations, stakeholders highlighted the importance of taking a holistic approach to the issue of children's access to online pornography.

Such an approach should consider the roles various participants across the ecosystem can play to prevent and reduce harm in all places where children may be at risk of encountering online pornography.[87] This ecosystem includes both child[88] and adult internet users, the adult industry, governments, NGOs, academics, researchers, and civil society groups. It also includes the many intersecting layers of the online industry, such as age assurance and other safety technology providers, as well as the device a person uses to access the internet, the service that provides their internet connection, and the platforms where content is shared and viewed. Noting the complex relationships between these different entities, a holistic approach should also consider how regulation of one part may have flow-on effects (intended or not) elsewhere.

A holistic approach considers the rights, experiences, and motivations of children, and the different situations and reasons children encounter or seek out pornography. Children's experiences online change as they age. They use the internet for different purposes and have evolving capacities and increasing independence to participate, learn, and explore online. Different complementary measures to address access to and the influence of pornography may be suitable for different ages and developmental stages.

Consideration should also be given to the roles, responsibilities, and rights of parents and carers, educators, and other adult users of the internet. This includes those who create and perform in pornography, the NGOs and researchers working on these issues, and the range of different products and services that make up the online industry. The human rights implications for both children and adults of measures which seek to restrict children's access to online pornography should be considered.[89]

In addition, it is important to consider some of the emerging developments which may create new and more visceral harms as well as new opportunities for preventing and mitigating harm to children from online pornography. This includes the use of generative AI and deepfake technologies to produce synthetic online pornography,[90] as well as the potential that the metaverse[91] and immersive technologies may create high-impact, hyper-realistic sexual experiences online[92] which blur the lines between content and conduct.

It is eSafety's position that any technical measures introduced to address this issue must also be supported by educational measures for children and the adults in their lives. Educational measures are discussed in the 'education' section below.

Experiences of under 10s and relevant complementary measures

According to eSafety's research from 2018, of the 81% of Australian parents with pre-schoolers that use the internet, 94% reported their child was using the internet before the age of 4.[93] It is therefore critical to start teaching children and the adults in their lives about online safety from the earliest years.

eSafety's research with 16-18-year-olds found 8% of participants who had seen online pornography first did so when they were under 10 years old. This is broadly consistent with other evidence across the literature, which shows it is relatively uncommon for children to encounter pornography before the age of 10. However, consultation participants reported anecdotal experiences of children viewing or sharing pornography as young as 6 or 7 in a school setting, and there is a perception the age of children encountering online pornography is getting younger. As highlighted above, research is very limited as to the nature of children's access to online pornography at this age due to ethical and other limitations in surveying children under the age of 16.

Noting that some children have accessed online pornography by this age, some stakeholders suggested late primary school (ages 8 to 10) is a suitable time to start having conversations with children about online pornography in a developmentally appropriate manner, using less explicit language than may be used for older cohorts.

Many children at this age are using shared family devices. This creates opportunities for supervision, discussions about online safety, and implementation of a range of safety technologies which can prevent children from encountering online pornography (in addition to – or in place of – any age assurance measures which may be voluntary, or mandated). This includes filters, safety and privacy settings, and parental controls.

Filters are used to screen out certain types of content, such as pornography. Safety and privacy settings can include limits on the types of activities a user can engage in, who they can connect with and what type of information about them is shared with others. Parental controls can include filters and safety settings, as well as the ability to supervise use and provide or withhold permission to do certain things, such as download a particular app or visit a particular site. These technologies may be built into products and services or provided by a third-party in the form of software or hardware such as a smart router. They may be on or off by default, and they may be available for free or by payment. They can be applied at various levels, including device- or operating system-level, browser-level, account-level, or network-level.

These technologies can also interact with other layers in the digital ecosystem in different ways. For example, filters may be more likely to capture pornography sites which apply meta tags such as the Restricted to Adults (RTA) label created by the Association of Sites Advocating Child Protection (ASACP).[94] In addition, the operation of third-party safety technologies may be impacted by the settings, policies or any changes to the settings or policies of operating systems, browsers, app stores, and the like. The second phase of the industry codes or standards which are to be developed under the Act will cover eight sections of the online industry. It will need to consider the connections between different technologies and be informed by this roadmap and its background report. For example, it will be important that search engine services do not inadvertently prioritise links to those pornography sites which do not require assurance over those sites which do employ such steps and where there may subsequently be a relatively high bounce rate[95] and low dwell time.[96]

As part of its independent assessment for eSafety, Enex Testlab assessed two third-party software filters and two smart router filters against several different lists, including a list of sites containing pornography. Overall, filters were assessed as a relatively mature and effective option for preventing access to online pornography, particularly for younger children who are less likely to try to circumvent these technologies and for whom over-blocking of information is less of an issue.

However, while these technologies can be effective, there are also challenges. According to recent research commissioned by DITRDCA, 45% of parents and carers in Australia do not use any parental controls.[97] The research found "it was evident that not all parent/carer participants were aware of the full range of parental controls available. This indicates that online safety education and support for parents is a broader, ongoing need".[98] Other potential barriers to applying these options include low digital literacy and the cost of these technologies.

Government and the online industry both have a role to play in addressing these challenges. Notably, France recently introduced legislation for parental control tools to be built into all smartphones and internet-connected devices sold in France at no additional cost, with parents prompted to switch it on for devices provided to their children.

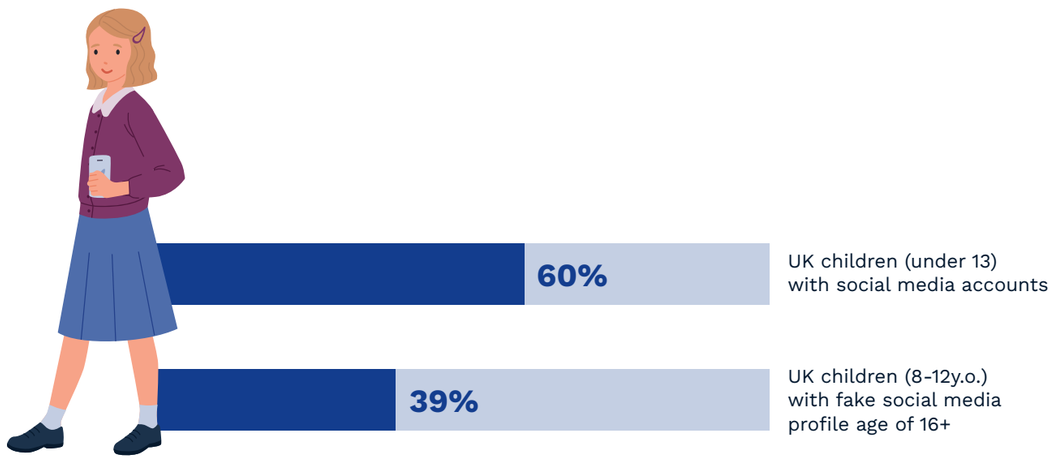
Experiences of 10-13-year-olds and relevant complementary measures

eSafety's research found 39% of 16-18-year-old participants who had seen pornography had done so before they were 13.[99] Those who encountered online pornography before the age of 13 were more likely than others to say they subsequently encountered online pornography frequently (several times a day). This was also reflected in UK research which found that those who viewed online pornography at age 11 or younger were more likely to access pornography frequently.[100]

Children in this age group may be more likely than younger children to have unsupervised access to devices. At this age, children generally are not permitted to have their own accounts for many online services, including social media services, which may be a conduit for online pornography. However, enforcing a relevant minimum age requires services to employ effective age assurance measures. While many online services have minimum ages of 13+ to sign up for accounts, they often rely on users to self-declare their age, and research has found many children provide false ages. UK research found 60% of children under the age of 13 who use social media accounts have their own profiles, despite not being old enough – and 39% of children aged 8-12 with a social media profile have a user age of 16+.[101] This means age-specific safety measures will not be properly enabled and therefore will not be effective.

Accordingly, online services should – and some do[102] – employ other measures to detect underage users. This can include AI profiling[103] and user reporting mechanisms[104] to identify potential underage accounts. This may result in accounts being suspended until the user verifies their age, for example, by providing a hard identifier such as government ID.

While age gates based on self-declaration present no barrier to those who want to evade them, it is important to acknowledge they can, in some circumstances, serve an important role in preventing unintended access to online pornography. For example, if a user follows a link to a site not knowing what it contains, the age gate requires confirmation from the user they wish to pass the age gate to enter the website and see the content.



[Ofcom, Children's Online User Ages Quantitative Research Study, October 2022]

Consequently, during consultation, some stakeholders suggested this creates an important signal for children to understand the content is not meant for them and provides a point of reflection and conscious decision to continue. This reduces unintentional and unwanted encounters and may deter some children from proceeding to view the content. Notably, of the top five most accessed pornography sites from Australia, only xHamster.com is age gated.

Unintentional and unwanted encounters can also occur through messaging of links, images, or videos, including in group chats. Messaging services both within and outside social media platforms should build in features to safeguard against this. For example, Apple allows parents to turn on tools in the Messages app to warn children within their Family Sharing plan when receiving photos that contain nudity.[105]

In addition, the safety technologies discussed above – filters, safety and privacy settings, and parental controls – can continue to be applied at various levels for children in this age group, including at the account level if the child's age is properly configured (for example, on a Google account supervised through Google Family Link).[106] However, as children get older, it becomes more likely they may seek to bypass safety features put in place by parents or carers.

Parents may also elect to disable features if they feel their children have outgrown them. For example, in the UK, major internet service providers (ISPs) provide customers network filters to block adult or illegal content.[107] In a 2022 paper, Ofcom found that although 61% of parents are aware of network-level internet filtering tools provided by ISPs, only 27% choose to use them.[108] Some stakeholders felt filters and parental controls tend to take a rigid, heavy-handed approach that leans toward prohibiting questionable material for anyone under the age of 18. They argued there would be benefit in calibrating different experiences and permissions for children as their capacities evolve rather than creating the same experience for all children from 0 through 17.

Family Friendly Filters

The Family Friendly Filters program is operated by the Communications Alliance, an association which represents the Australian communications industry. The aim of the program is to test, certify and promote high quality filter products to the public to encourage safer internet access for children and families.

All filter products are eligible to apply to be part of the program. In order to be certified, a filter must undergo independent testing to ensure it meets criteria intended to correspond to the national Classification Guidelines for films and computer games. These include effectiveness, ease of use, configurability, availability of support, and agreement by the filter company to update the filter as required.

There are four levels of classification for certified filters which align to age groups depending on their risk of under-blocking age-inappropriate material and of over-blocking age-appropriate material:

- **Unclassified: Recommended for people 18+**
- **Class 1: Recommended for children over 15 years of age**
- **Class 2: Recommended for children between 10 and 15 years of age**
- **Class 3: Recommended for children under 10 years of age**

The approach of independently testing products and classifying them according to age segments has potential to address the previously identified need to adjust safety settings over time as a child grows and develops. However, it is unclear to eSafety how well known the program is among the Australian public, as Communications Alliance does not have data on consumer awareness and uptake.

Stakeholders had differing views about the appropriate age to begin talking to children about online pornography. However, many felt this education needs to begin in upper primary school, in an age-appropriate manner, given the early age of first encounters. This is discussed in more detail below. International guidance developed by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) suggests discussions of online pornography literacy and gender stereotypes should begin from ages 9-12.[109]

Experiences of 13-15-year-olds and relevant complementary measures

eSafety's research found 47% of 16-18-year-old participants who had seen online pornography first encountered it when they were 13, 14 or 15 years old. Altogether, 86% of the participants in our survey who had seen online pornography had done so before the age of 16.[110] This is broadly consistent with other Australian research, which found the average age of children first viewing online pornography was 13.[111]

According to Australia's National Research Organisation for Women's Safety (ANROWS), from age 14+, viewing pornography may be an age-appropriate sexual behaviour.[112]

This was echoed in our consultations. However, many stakeholders pointed out there is an important distinction between children displaying an age-appropriate interest or curiosity in certain material, and that material being age-appropriate for them to view.

At this age, more children are using their own devices, and often doing so without supervision. At 13, children can create their own social media accounts, according to the terms of service or community rules of most major services. Some 13+ online services allow pornography (for example, Discord, Reddit, and Twitter)[113] while others do not (for example, Instagram, Facebook, Snapchat, and TikTok).[114] Children report regularly seeing pornography across both services that do and do not allow it. Common places reported in our survey of 16–18-year-olds included social media feeds (35%), ads on social media (28%), social media messages (22%), group chats (17%), and via social media private group/pages (17%).[115] According to recent research from the UK Children's Commissioner, Twitter is the online platform where 16-21-year-olds were most likely to have seen pornography. Of those who had seen pornography, 41% reported having seen it on Twitter. Dedicated pornography sites were the next most likely platform (37%), followed by Instagram (33%), Snapchat (32%), and search engines (30%).[116]

Services which do not allow pornography

If a service does not allow pornography, this should be clearly set out in the terms of service or community rules, and such terms or rules should be enforced. This requires services to have accessible and effective mechanisms for users to report pornography they encounter on the service, as well as proactive content detection tools. As part of its review, Enex Testlab assessed an artificial intelligence (AI) content moderation service that can be configured with a range of modules which detect and moderate various types of content and activity for the online services which purchase it. This includes detecting underage users (for example, those who have created accounts with a false age) as well as detecting sexual content, depending on the client service's configurations. Based on interviews with three clients running large online services, Enex Testlab concluded the technology is successfully deployed in the marketplace with good results.

Services which do allow pornography

If a service does allow pornography, but also allows users under the age of 18, it should put in place effective safeguards to prevent younger users (and those who do not wish to see pornography) from encountering this content. This requires more robust age assurance measures than self-declaration, coupled with age-appropriate safety features enabled on accounts by default so pornography is not recommended to, or accessible by, younger users.

Some services rely on the user community to assist with moderation efforts. For example, users tag adult content as 'sensitive' or 'not safe for work' (NSFW). In these circumstances, rules need to be enforced, with consequences for users who fail to follow tagging requirements. Such tools should be properly calibrated in consultation with the user community, so they meet users' needs and avoid over-blocking (especially of marginalised users). This will increase the likelihood of user uptake. For example, Twitter initially introduced a requirement for users who regularly share adult nudity and sexual behaviour to mark their accounts as sensitive, which removes their content from recommendations to general audiences and places it behind warning messages. Following feedback from the user community that people may be disincentivised from marking their entire account as sensitive since this could limit their reach to new audiences, Twitter introduced the option to mark individual Tweets as sensitive to provide a more targeted and proportionate approach and increase user compliance with the rules.[117]

Services for the purpose of pornography

If a service is dedicated to online pornography, it should have a very clear 18+ policy and meta tags, such as the Restricted to Adults (RTA) label, should be applied to make sure the site is blocked by any filters that may be in place for children. All explicit content should be placed behind an age gate, rather than on the landing page, and videos should not auto-play. Age assurance measures should be in place to confirm users are over 18.

There is a clear concern people may simply click away from a site or close a service if they are uncomfortable with the age assurance measures it applies and seek the same or similar content somewhere else. In our consultations, stakeholders emphasised that measures which create too much friction have the potential to deter users from accessing compliant sites. Instead, they may follow the path of least resistance toward sites which do not comply with age requirements – and may also contain more extreme and harmful content.

Accordingly, consideration should be given to complementary interventions in other parts of the digital ecosystem to prevent a child from landing at a pornography site in the first place, as well as preventing non-compliant sites from being surfaced at the top of search results.

The role of online search and other gatekeepers

Most visits to websites start with a search engine. Semrush data obtained in February 2023 indicates there are more than 18 million monthly Australian searches for the top five most visited pornography websites. Of the 16-18-year-olds we surveyed who had seen online pornography, 59% said they had intentionally searched for it.[118] Search engines can therefore play an important gatekeeper role in reducing children's access to this content via search. Google SafeSearch, which hides sexually explicit content from Google search results by default for certain accounts, and SafeSearch Blur, which blurs explicit media by default for all users, are good practice examples of complementary measures.[119]

Other entities within the digital system with the potential to play a similar gatekeeper role and significantly influence user safety include app stores,[120] browsers,[121] and device manufacturers.[122]

However, measures applied to protect children should not unduly restrict the rights of adults to create, access, and share lawful content. In addition, any such efforts should be balanced against the need to preserve age-appropriate access to sexual health and wellbeing information and support.

Age policies for parental controls

While parents and carers can continue to use filters, safety and privacy settings, and parental controls for teenagers, at this age, their children may be likely to bypass those features, and might have legitimate reasons for doing so. For example, stakeholders raised risks associated with the use of parental controls in families where sexuality is not discussed in an open and supportive manner or where violence or coercive control is involved.

Notably, some companies have made policy decisions about the age at which children can decide for themselves when to end parental supervision, subject to local laws which may specify a higher age for children in a particular country. For example, Australian children whose Google accounts are supervised through Family Link have the option to turn off parental supervision or to allow their parent to continue managing their account at age 13.[123] Parents do not have the ability to override this decision. Examples of countries that have established higher minimum ages for children to manage their own accounts include Austria, Chile, Cyprus, Italy, South Korea, and Spain (age 14), Czech Republic, Greece, Serbia, and Vietnam (age 15) and Aruba, Croatia, Germany, Ireland, Netherlands, and Slovenia (age 16).[124]

Similarly, when an Australian child turns 13, they are permitted to maintain their own Apple ID account without participating in Family Sharing, regardless of their parents' views.[125] However, children may be incentivised to continue Family Sharing if their parents are paying for their access to services like Music and TV. In addition, parents can lock the Content & Privacy Restrictions within the Screen Time app on a child's device by protecting them with a passcode linked to their own Apple ID and password, regardless of the age of the child.[126]

In eSafety's research from 2018, parents' views on appropriate interventions also reflected the evolving capacities of their children. Parents of children between the ages of 13–17 were more likely to favour education (81% versus 58%) and less likely to favour monitoring (71% versus 89%) than parents of children aged 6–7 years about issues of online pornography.[127]

Experiences of 16-17-year-olds and above and relevant complementary measures

eSafety's research found 10% of participants who had seen online pornography first encountered it when they were 16 years old. Only 4% were 17 or 18 when they first encountered it, as the vast majority had already seen it by then.[128]

As noted above, in most states and territories in Australia, the age of consent for sex is 16.[129] In our focus groups with 16-18-year-olds, and eSafety's survey of 16-18-year-olds, we found one in two respondents think the age of access to online pornography should match the age of consent. eSafety notes that developments in the metaverse and immersive technologies come with a blurring of lines between content and activity, as our online interactions shift from exchanging distinct pieces of content to live and synchronous interactions. In the online pornography context, this could precipitate a change from simply encountering sexual content to engaging in sexual experiences, raising questions about the applicable minimum age and necessitating far more robust age assurance measures to protect younger children from exploitation and abuse.

By age 16 or 17, most Australian children have received some form of sexuality and respectful relationships education, but there are significant gaps. Some children are not likely to get this information at home or at school, and where they do get information, it might not be relevant or inclusive. Teenagers' ability to access judgement-free information independently or from frontline workers is discussed in the 'education' section below.

Unintentional access

One of the themes arising from both the quantitative survey as well as focus groups with 16-18-year-olds was the pervasiveness of online pornography and the feeling of constantly seeing it unintentionally. Participants typically felt very negatively about unintentional encounters with online pornography, describing them as unwelcomed, unwanted, and disempowering.

Unintentional access occurs through searches for other content, pop-ups, group chats, and social media feeds. Recommender systems can contribute to the inappropriate content and accounts being displayed to children unexpectedly, especially where weak age assurance measures lead to accounts failing to reflect their true age.

Research submitted to eSafety recognises sexual agency, or being in control of one's own sexuality, as an important domain of healthy sexual development for children and young people.[130] This was echoed by participants in our survey and focus groups, who emphasised young people's ability to make decisions about what is best for them regarding online pornography. The emphasis they placed on having agency over viewing pornography was centred both on being able to choose when they intentionally view pornography and being able to choose when not to see pornography and avoid unintentionally encountering it in locations outside of pornography sites.

Minimising the potential for unintentional encounters with online pornography – and giving users control over their experience and what they see – is consistent with a Safety by Design approach, which aims to create a safer and more inclusive digital ecosystem, particularly for those most at risk of harm.

Safety by Design and user empowerment

Safety by Design encourages industry to anticipate potential harms and implement risk-mitigating and transparency measures throughout the design, development, and deployment of a product or service.[131] This approach seeks to minimise any existing and emerging harms that may occur, rather than retrospectively addressing them after they occur. A key principle of Safety by Design is user empowerment and autonomy.

There are a range of good practices that can be applied to give effect to this principle, including enabling users to identify the types of content they do and do not wish to see, and to alert the service if they are being served content they do not like.

For example, xHamster.com, a popular pornography site, enables users who have watched 10 or more videos to reset their recommendations. This clears a person's viewing history, which could reduce the potential for unwanted content silos of increasingly extreme pornography. Similarly, Instagram, a social media service which does not allow sexual activity, provides users with a level of control over their recommender system through feedback loops allowing them to flag types of sensitive content they do not want to see in suggested posts. This includes content that may be sexually suggestive.

In March 2022, Google announced it was using advanced AI technologies to improve its understanding of whether searchers are truly seeking out explicit content, helping to reduce a user's chances of encountering these results unintentionally. Google announced this had been especially effective in reducing explicit content for searches related to ethnicity, sexual orientation, and gender, which can disproportionately impact women and especially women of colour.[132]

Safety expectations which are already in place, and avenues to promote or mandate complementary measures

As set out above, the Act already has mechanisms in place to help prevent children from encountering online pornography. For example, in addition to the specific Expectation in relation to preventing children from accessing X18+ or R18+ material, there are broader Expectations to have and enforce terms of use, to provide users with clear and readily identifiable reporting and complaints mechanisms and to ensure safe use.

This report will inform future reporting notices to be given by eSafety to online services and any further eSafety guidance issued in relation to the Expectations. It will also inform the development of the second phase of industry codes or industry standards (discussed above) which will focus on measures to prevent and address children's access to pornography (and other high impact content).

Finally, it can inform eSafety's broader engagement with industry, including our Safety by Design activities.

Roadmap

eSafety's proposed next steps

6. Industry engagement and Safety by Design:

- The findings of this report will inform eSafety's engagement and sharing of good practice with the online industry, including through our Safety by Design activities and our Tech Trends and Challenges papers.
- Through the Safety by Design initiative, eSafety will continue to raise industry's awareness of the harms associated with children's access to online pornography and provide practical information about appropriate interventions.
- eSafety will continue to make sure Safety by Design is future-focused by updating existing materials for emerging technologies such as immersive environments.

7. Basic Online Safety Expectations and the development of industry codes or industry standards

- The complementary measures outlined in this report can help inform reporting notices and guidance to be issued by eSafety relating to the Expectations. The measures can also help inform the second phase of industry codes or industry standards which will focus on measures to prevent and address children's access to pornography (and other high impact content).
- These measures include:
  - the provision of clear and relevant safety information, accompanied by targeted awareness raising
  - the provision of filters, safety and privacy settings, and parental controls
  - clear policies in relation to online pornography and enforcement of those policies
  - a clear minimum age to use the service and enforcement of that minimum age through age assurance mechanisms at first access/ sign up, as well as ongoing measures to detect underage users in appropriate circumstances
  - the application of age gates and pornography-free landing pages
  - the application of age-appropriate safety and privacy settings to the accounts of younger users
  - accessible and effective mechanisms to report (unrestricted) online pornography
  - proactive content detection and moderation technology, which is subject to appropriate and accessible appeals processes and continuously improved in consultation with the user community
  - the provision and enforcement of tools for the user community to apply tags to sensitive content and accounts, and effective measures to make sure they are not promoted to younger users
  - the provision of features for users to control their experience and the type of content recommended to them
  - efforts to minimise unintentional encounters, for example, by improving accuracy of search results and blurring sensitive content
  - ongoing investment and innovation in development of tools and the above measures transparency reporting.
- Additional considerations to inform these processes include:
  - the ability to calibrate different experiences and permissions for children which can be adjusted as their capacities evolve
  - whether Australia, like other countries, should consider applying a higher minimum age than 13 for children to override parental supervision on their accounts
  - the cost of safety measures, and how much of this cost should be borne by consumers versus industry
  - whether safety measures are in-built and on by default
  - how to reduce any barriers to third-party safety measures
  - the inter-relationships between various entities within the digital ecosystem, and the opportunity to leverage these connections to improve safety outcomes and reduce the potential for unintended consequences.

eSafety recommends the Australian Government

3. Fund eSafety to:

- Develop bespoke Safety by Design resources on good practice in relation to age assurance and complementary measures to create safe and age-appropriate online spaces.
- Establish an online safety tech centre which serves to support parents, carers, and others to access, understand, and apply safety technologies that work best for their family's circumstances as one part of a holistic approach to online safety. This centre could also support schools in relation to the use of safety technology, in partnership with state and territory governments, as discussed in the next section.

4. Conduct further work to:

Determine the extent to which the cost, availability, awareness, or any inherent practicalities associated with safety technologies such as filters and parental controls present a barrier to their uptake by Australian families.

Education and awareness raising

Activities for awareness raising and education for the public

The importance of education was highlighted frequently in the research submitted to, and conducted by, eSafety, as well as in the consultations held across nearly all stakeholder groups – including children and young people themselves.

Consultations and research highlighted that a range of educational measures are necessary to address the harms to children associated with online pornography. There is a wealth of existing initiatives and good practice to build on in this space, and an array of new work commencing – particularly in the areas of consent, respectful relationships, and prevention of gender-based violence.

The measures should:

- support children and young people to understand the content they see online, including online pornography, critically think about its purpose and the narratives it contains, and know how to seek help or help themselves when they see unwanted content which makes them feel uncomfortable
- equip trusted adults in children's lives, including parents and carers, educators, frontline workers, and others who work with and support children and young people with the skills and knowledge to have conversations with children about online pornography
- address some of the specific harms associated with online pornography, including by providing inclusive sexual education (reducing the need for children to seek out other sources which are not intended to be educational) and addressing concepts such as consent, safe sexual practices, and respectful relationships.

Many factors can impact the potential for online pornography to harm children. There was greater agreement among the stakeholders we consulted about the potential harm to younger children as opposed to older teens. Younger children are more likely to lack the capacity, context, and support to critically analyse what they are seeing and temper its influence. Any measures must reflect the evolving capacities, needs, rights, and best interests of children across different ages and stages.

eSafety's research indicates educational measures and awareness raising activities should cover:

- how age assurance tools work and what measures are in place to protect children's (and others') safety, privacy, and security
- how people can access and apply safety technology and tools, such as parental controls and search filters (this was raised as a particular concern for parents in submissions and consultation).

There are opportunities for government and industry to do more to raise awareness of, and to educate people on, the use of existing and emerging safety tools. Educational and awareness raising activities should target specific audiences with tailored content.

For parents and carers

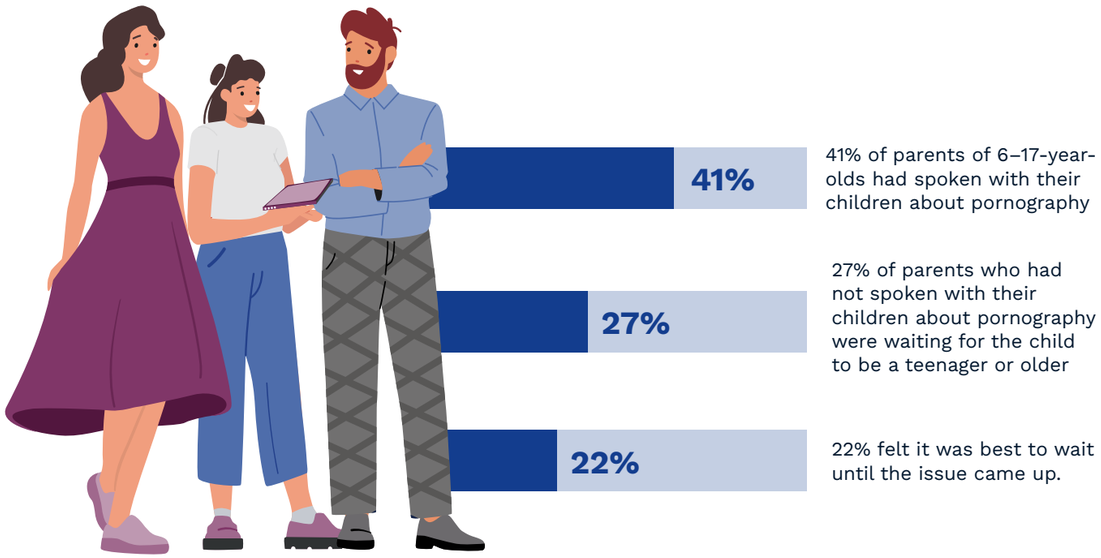
It is important to equip parents and carers with the right information and tools to have sufficient information to confidently address these issues.

In 2018, eSafety's research with parents of 6–17-year-olds found only 41% of parents had spoken with their children about pornography, 27% of parents who had not spoken with their children about pornography were waiting for the child to be a teenager or older and 22% felt it was best to wait until the issue came up.[133] Our 2022 research with children reveals it is too late to wait until teenage years, as many children see online pornography at 13 or younger.[134]

It is important to inform parents and carers how to have conversations about pornography in a helpful, supportive, and shame-free way to prevent and mitigate harm. The eSafety parent portal provides scripts to help parents have difficult conversations, including on how to speak with children about online pornography at different ages and developmental stages.

A third of the young people we surveyed said parents are not equipped to support young people to manage the impacts of online pornography (41% of LGBTIQ+ young people) and 38% said education should be provided to parents and carers so they can better support young people with this issue.

Research demonstrates that where children's encounters with pornography result in harm, some of that harm stems from the subsequent negative reactions of trusted adults (such as anger or shame) as opposed to the material itself.[135] This may include families where sex and sexuality are not discussed in an open and supportive manner, or where family, domestic, or sexual violence is a factor in the home. Education for parents and carers needs to be tailored to meet the needs of different families, including by accounting for cultural and linguistic diversity, and to address potential barriers to constructive dialogue.



eSafety's existing advice for parents and carers about choosing and using parental controls includes guidance on our website, an information video, and factsheets (Parental controls in social media, games and apps, and Parental controls on devices and accounts). Support for parents and carers is also available from online safety education providers who have been endorsed under the Trusted eSafety Provider Program. NGOs supported through eSafety's Online Safety Grants Program also offer other sources of inclusive citizen-focused online safety education resources for parents and carers.

eSafety also provides advice and resources to support parents and carers to start age-appropriate conversations, including 'Online porn' and 'Hard to have conversations'. This information is segmented by developmental stage, including advice targeted to parents and carers of young people aged 5-12. We worked with Dr. Justin Coulson, parenting expert on this guidance. Many other organisations provide similar advice.

Further work and awareness raising about the availability of these tools and information is required. One of the specific areas of need identified in submissions and consultations, especially for parents of younger children, was education and information for parents and carers on how to access and apply safety technology and tools. Stakeholders involved in our consultations highlighted that parents who are less comfortable using technology can be more restrictive of their children's internet use due to fears of online harms, including accessing pornography. This can result in children and young people missing out on beneficial educational content and social interactions online.

In our consultations, online services and industry associations highlighted a variety of parent resources provided by social media services, search engines, internet service providers, telecommunications companies, and others. Some stakeholders pointed out challenges in reaching parents with this information.

They pointed to the benefits of partnering with NGOs and other specialist organisations as well as facilitating parent-led, peer-to-peer education and information sharing, including through parenting groups on social media. This was an area where many stakeholders felt government could help, including potentially through the creation of an online hub for parents to access information and online safety tools or programs.

It was also noted that parent's digital literacy and low awareness of these technologies are only some barriers to their uptake. Other barriers include cost, challenges with installation, and parental perceptions about their efficacy and appropriateness.

Resources for parents and carers should equip them with the information and skills needed to have conversations with children about online pornography (including the nature of mainstream online pornography and why and how children may access it), as well as offer advice on how to talk to and support their children – both educationally and through technical measures.

eSafety recognises there are challenges in reaching parents with online safety information, a point noted by many stakeholders. More should be done to make parents and carers aware of existing resources available to them. There is scope to explore pathways to increase parental awareness about pornography and its harms, including encouraging uptake of available online safety tools, such as through a national public education campaign, or working with specialist organisations.

For educators

Like parents and carers – and in line with good practice frameworks[136] – educators should be equipped to have conversations with students about online pornography in a way that is safe and supportive for all parties. This is important not only to make sure educational messaging about pornography, sex, consent, and respect is delivered in an effective way, but also to prepare the school and its staff to address any pornography-related incidents that arise either at school or within the school community.

The education authorities and providers we consulted identified incidents at schools involving students' use of pornography. They observed an increase in reports from teachers and students of peer-to-peer sharing of online pornography and noted this was happening in primary schools as early as year 1 or 2.

While some teachers and school wellbeing staff are highly trained and well equipped for these discussions, consultation participants reported that the level of confidence in discussing these issues with students varies widely. Many feel inadequately prepared and resourced to discuss pornography with students. Tailored material is needed to assist them in having safe and age-appropriate conversations.

Professional learning and guidance for educators should include information on the safety tools available to prevent access to online pornography, and methods for integrating modern online pornography discussions into sex education and respectful relationships topics.

This can be provided to educators through pre-service teacher training, ongoing professional development courses, or resources and communities of practice. Some educators said it may be more effective to build this content into ongoing professional development rather than pre-service training curriculum, as there may be more opportunities to update content to reflect any changes. Stakeholders also encouraged content which helps educators speak with parents and carers, as well as students. Such training should also be bolstered through school policies and procedures to support educators and create a safe and inclusive culture.

Existing measures, gaps and opportunities for improvement, and good practice in training delivery are explored in our background report.

In addition to having policies and procedures in place (e.g. technology usage agreements and codes of conduct), stakeholders discussed some of the technological approaches to preventing students' access to pornography at school or on school-based devices. Measures included device-level filters, network-level filters, proactive scanning for certain language, and individual incident alerts on the school Wi-Fi network. It was noted content filters and restrictions could either be applied to the whole school population or by year group to align with age appropriateness.

Challenges implementing these measures were also identified, such as students using mobile hotspots and personal devices (not subject to school controls) to avoid the school's content filters and restrictions.

Stakeholders told us even the most robust safety settings and controls will not provide a 'silver bullet' solution, highlighting the importance of a more holistic approach. They raised the importance of having robust and evidence-based policies, procedures and resources for students, staff, and parents and carers to prevent and address pornography-related incidents involving the school community. In addition to promoting eSafety's existing online safety education resources, there is the opportunity to leverage insights from the roadmap research, consultation process, and the background report to develop further evidence-based resources for teachers and schools.

For frontline workers and others working with children

Frontline workers, and other professionals working with or providing care to children and young people, should be provided with resources and guidance to address online safety issues in children and young people's lives. This includes discussing online pornography in an informed, safe, and judgement-free way with justice and community services, allied health, out-of-home care, and flexible learning environments.

The role of people working with children is potentially more important for those children and young people who have experienced instability or uncertainty in their home environments. This may be particularly true in situations where they have already developed a potentially unhealthy relationship with pornography or are at risk of doing so, including those who have engaged in harmful sexual behaviour or been subjected to sexual abuse.

Some young people may be more likely to seek support and information from other sources. Young people surveyed who speak English as a second language at home indicated they were more likely to seek information and advice about online pornography from support services, compared to young people who do speak English at home.

Consultation participants felt out of home care, youth, and allied health workers in particular should be upskilled on how to respond to a broad range of online safety issues – including access to pornography and in identifying the signs a child may be having negative online experiences. This is particularly relevant, as issues relating to online pornography can cut across many topics, including body image, mental health and wellbeing, relationships, and sex, sexuality, and sexual health.

eSafety has existing resources available for frontline workers, including the eSafety Frontline Worker Training and Association of Children's Welfare Agencies (ACWA) Resources for Out-of-Home Care Workers. There is the potential to incorporate information about the impact and prevalence of online pornography, age assurance and other online safety tools into this training. This is especially so for residential care, and youth and allied health workers, who consultation participants felt should be upskilled on a broad range of online safety issues – including access to pornography.

For children and young people

In our research, young people were critical of the way sex and relationships education was delivered. This is broadly consistent with other recent Australian research which finds sex education in schools is delivered inconsistently and with varying levels of efficacy.[137] However, 16-18-year-olds in our research also saw a role for inclusive, stigma-free education in mitigating the potential harms of pornography and in supporting them to navigate encounters with online pornography.

eSafety consulted with children and young people, academics, educators, and child rights experts on what education for children about online pornography should look like and how it should be best delivered. eSafety also mapped out the existing resources. This is further explored in our background report. There was broad agreement programs and resources should be underpinned by established good practices in online safety, sexuality, respectful relationships, and pornography education.

Education for children and young people should:

- start with foundational skills at an early age and build over time
- be informed by best practices
- involve young people's voice, perspectives and participation in design and delivery
- be inclusive, strengths-based, and stigma free
- use a whole-of school approach
- be integrated and co-ordinated
- include support outside of the school environment.

Age-appropriate education about the concepts of consent, respect, and online safety are largely accepted as being necessary from the earliest ages. Skills which support young children develop resilience, respect, critical thinking, help-seeking, and protective behaviours online are foundational skills which can be built on in subsequent learning to address specific risks and harms.

Stakeholders offered different perspectives on when it is best to include pornography-specific education. There is discomfort and uncertainty among parents and educators about when and where to have conversations about online pornography with younger children, in a way that promotes their best interests. eSafety heard many schools are hesitant to discuss online pornography, particularly in primary school, due to concerns about appropriateness or student wellbeing. This also points to the need for resources for schools and educators to support them to respond to pornography related incidents and teach skills relevant to these issues.

In 2020, eSafety commissioned a Best Practice Framework for Online Safety Education, which establishes a nationally consistent approach to delivering high quality online safety education programs in Australia. It includes clearly defined elements and effective practices to support a whole-of-school approach for creating a safe online environment.

The review which supported the framework suggests effective online safety programs about online pornography include sex education; address the messages boys and girls take from pornography and how they differ and influence their relationships; and consider gender equality, drivers of gender-based violence, sexual harassment, coercion, consent, and victim blaming.

Youth participation and co-design can help to make sure messaging is relevant, relatable, authentic, and effective. Youth engagement is also vital to make sure the content is meeting young people's needs. Our research found 42% of the 16-18-year-olds surveyed (and 58% of LGBTIQ+ respondents surveyed) felt current education about sexuality and relationships does not meet young people's needs.[138] Research and consultations pointed to the importance of providing balanced and non-judgemental education and support for children and young people to navigate these issues.

Both children and young people and adult experts emphasised it can be helpful to incorporate a collaborative, peer-to-peer approach to education on these topics, as young people often turn to their peers for support and advice about sex and relationships.

Education should allow for an exploration of diverse perspectives in a way that is constructive, trusting, and respectful.

The needs of diverse communities

In one study, one third of LGBTQA+ students in secondary schools reported never having any aspect of LGBTQA+ people mentioned in a supportive or inclusive way during their relationship and sex health education.[139] A strong theme in the consultations, backed up by other evidence, was some pornography can be validating and affirming for those who do not see themselves represented in mainstream media and sex education, particularly LGBTIQ+ young people.[140]

Children and young people with intellectual disability or who are neurodivergent may likewise find their sex and relationships education lacking in representation of their experiences, lacking in support for their specific needs, or simply lacking from their education.[141] Tailored resources about online pornography can be helpful for these young people and their families.[142]

Education which applies a gender lens and is inclusive of all sexualities can increase resilience to sexist and violent scripts commonly found in mainstream pornography. It may also reduce the likelihood that LGBTIQ+ young people find their sexual education inadequate[143] and seek out information from other sources such as pornography.[144]

As outlined earlier in the roadmap and in our background report, there is a need for educational resources to be catered to the specific needs and circumstances of all children. Resources should enable educators and children to engage with these issues in a way that is culturally safe and inclusive. Stakeholders suggested the need for resources tailored for specific groups, such as First Nations children, LGBTIQ+ children, culturally and linguistically

diverse (CALD) children, and children with disabilities. These resources should support educators to understand the different contexts in which children access or engage with online pornography and how that affects their understanding of sexual identity, expression, and healthy relationships.

Need for consistency, flexibility, and coordination

A whole-school approach includes a supportive school climate, curriculum, and wellbeing teaching and learning activities, as well as robust policies and procedures, staff professional development, student voice and agency, and parent/carer, and community partnerships.

While some education sectors in Australia provide and support age- and stage- appropriate teaching and learning and resources for respectful relationships as part of a whole school approach, there is no consistent curriculum for respectful relationships in Years 11 and 12.

Our consultations pointed to multiple intersecting policy developments in different parts of the Australian Government and called for greater coordination across government and the creation of a national coordination mechanisms for respectful relationships education and policy. There is a wealth of existing initiatives and good practice to build on in this space, and an array of new work commencing – particularly in the areas of consent, respectful relationships, and prevention of gender-based violence.[145] There are also multiple areas of the curriculum where further education about online pornography can be integrated.

The Australian Curriculum

The recently updated Australian Curriculum (version 9), developed by the Australian Curriculum, Assessment and Reporting Authority (ACARA) following the 2020-21 Australian Curriculum Review, embeds online safety for Foundation to Year 10 across learning areas and the general capabilities. It is being implemented by states and territories according to their own timelines.[146]

Key curriculum learning areas encompass F-10 teaching and learning, with key concepts and skills explored in primary school being developed in complexity throughout secondary school. Relevant curricula include:

- Digital Technologies, Strands: Knowledge and understanding and Processes and production skills – focusing on privacy and security and the features of digital systems and tools. Students learn how to make informed and ethical decisions about the role, impact, and use of technologies in their own lives.

- Health and Physical Education, Strand: Personal, social, and community health – focusing on the knowledge, understanding, and skills needed to make healthy and safe choices online and offline (including protective behaviours, help-seeking, and upstander strategies) and to build and manage respectful relationships, including consent, communication, and decision-making.

  In February 2022, education ministers unanimously agreed to include consent-based education in the updated Health and Physical Education curriculum. This announcement followed a successful petition and campaign by activist Chanel Contos and her organisation, Teach Us Consent, which advocates for holistic sexuality education in schools, with sexual consent at the forefront, from a young age.

  In March 2022, it was announced that a national survey would be undertaken by the National Children's Commissioner and the Sex Discrimination Commissioner to explore consent education of secondary school students across Australia, and to provide benchmark data to gauge the impact of consent education in the revised Australian Curriculum.[147]

- Humanities and Social Sciences, English and The Arts – focusing on citizenship and developing critical thinking skills.

Key curriculum general capabilities include:

- Digital literacy, Element: Practising digital safety and wellbeing – in particular, students develop the appropriate skills and strategies to address online content risks and negative online social interactions. It assists students to adapt to new ways of doing things as technologies evolve and to protect their own safety and the safety of others.
- Critical and creative thinking – Critical thinking to teach students the skills of using information, evidence, and logic to draw reasoned conclusions and to solve problems.
- Personal and social capability – Supporting students to develop social and emotional skills and providing the foundation for students to navigate their relationships.
- Intercultural understanding – combining personal, interpersonal, and social knowledge and skills.

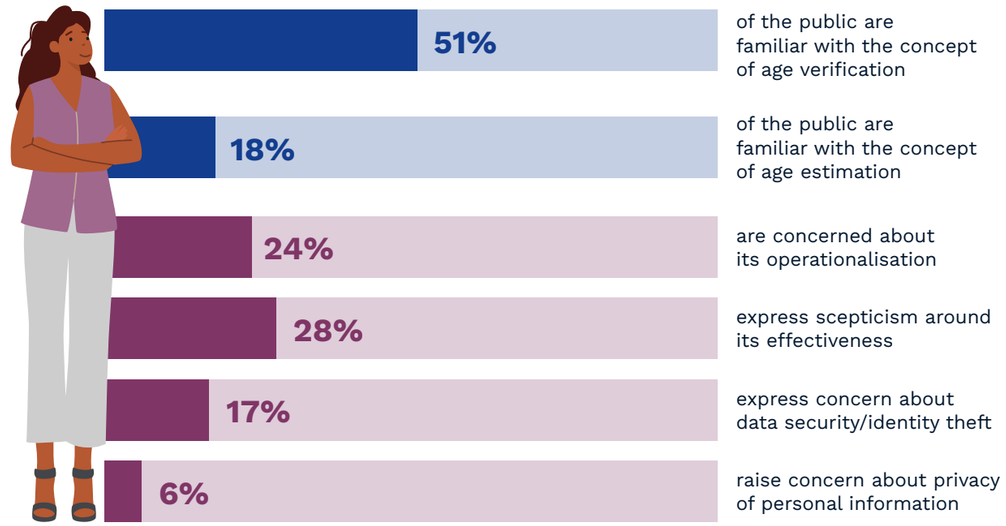
ACARA's curriculum connections for F-10 allow educators to draw connections across the dimensions of the Australian Curriculum. The Online Safety and Respect Matters curriculum connections (Version 8.4) support both the teaching and learning of online safety and address respectful relationships education through the curriculum schools deliver.

eSafety also heard through submissions and consultation there is benefit to programs targeting young people to provide them with independent and accessible means to receive robust sexuality and respectful relationships education. Community-based programs can support children and young people outside of mainstream schooling systems and could involve flexible learning centres, community health centres, out-of-home care, and in youth justice programs. Stakeholders also emphasised the value of having online sources of reliable, trustworthy, and age-appropriate information about online pornography so children can access it privately and independently.

Age-appropriate, inclusive, evidence-based, and stigma-free education about online pornography (and the related topics of online safety, sexuality, consent, and respectful relationships) are integral to addressing the harms associated with online pornography. Educational material should be co-designed with young people and informed by the specialist research mentioned earlier in this roadmap to make sure it is also tailored to and inclusive of cohorts currently underrepresented. eSafety can play a role in the development, promotion, and coordination of these measures.

Public awareness to support the implementation of age assurance

The introduction of any technical measures should be supported by communication and awareness-raising initiatives to bring the public along on the journey. eSafety's public perceptions research raised two main insights in relation to the public's knowledge and opinion of age assurance. First, when unprompted, only 51% of the public are familiar with the concept of age verification and 18% with age estimation.[148] Second, although 78% of people surveyed were supportive of the idea once they understood its meaning, 24% expressed concerns about its operationalisation, with 28% expressing scepticism around its effectiveness, 17% stating concerns about data security/ identity theft, and 6% raising concerns about privacy of personal information.



In response to this evidence, and if government decides to trial age assurance technologies, eSafety recommends this be accompanied by public education and awareness-raising efforts to build public knowledge and trust in the initiative.

This should include information about:

- what age assurance is: the various types of assurance available and the different levels of assurance required for various use cases
- what measures are in place to support user privacy, including:
  - what information is stored, collected, and used by age assurance providers
  - how the double-blind approach works
  - how information can be stored securely using a digital wallet and the ability to share an 'attribute' of identity
  - protections under relevant privacy legislation
- options to use alternative technical mechanisms if one technology provides inaccurate results or is not easy to access.

Education and awareness-raising efforts can be implemented by sharing findings online and holding events with subject matter experts. If a pilot proceeds to Beta testing with real users and environments, as was done recently in UK grocery stores,[149] this would also aid public engagement, facilitating trust across use cases, and promoting greater adoption.

Child- and young person-friendly information should also be available and informed by consultation with children and young people.

In addition, the existing resources which are available, and any new resources developed to fill gaps, should be supported through awareness-raising efforts. As noted above, there is a wealth of knowledge in NGOs, educational organisations, and across government. Mechanisms to coordinate these efforts could help raise the profile of existing effective educational resources and ensure consistency and continuity of good practice.

Roadmap

eSafety's proposed next steps

8. Resources for young people

- eSafety resources for young people will be co-designed, and internal and external subject matter experts will be consulted and engaged.

9. Coordination

- eSafety will continue working with the Australian Curriculum, Assessment and Reporting Authority (ACARA) to align eSafety's resources into relevant curricula and highlight resources on sexuality, consent, and respectful relationships.
- eSafety will, where appropriate, continue upskilling Trusted eSafety Providers and support online safety grants recipients with these issues.

10. Consultation

- eSafety will continue to consult with the eSafety Youth Council on the development and implementation of education and resources.
- eSafety will continue to consult with the National Online Safety Council (NOSEC) through reciprocal knowledge sharing.

eSafety recommends the Australian Government

5. Fund eSafety to:

- Review existing resources for alignment with the findings of the roadmap and background report and:
  - work with subject matter experts and communities to develop a suite of evidence-based, age-appropriate educational resources about online pornography for children and young people from a range of backgrounds and life experiences, such as First Nations children, LGBTIQ+ children, culturally and linguistically diverse (CALD) children, children with disabilities, and children who are especially at-risk.
  - develop complementary resources for parents, carers, and frontline workers to equip them to have age-appropriate conversations about online pornography and implement technological tools to prevent and mitigate harm associated with online pornography.
  - update eSafety's Toolkit for Schools and professional development resources for educators with information about online pornography, including strategies for preventing and managing pornography-related incidents and support pathways for students and families.
- Raise awareness of any new resources among key stakeholders and relevant groups.

6. Consider:

- The development of a mechanism for greater national coordination and collaboration of respectful relationships education, consistent with the Monash University report (Respectful Relationships Education in Australia: National Stocktake and Gap Analysis of Respectful Relationships Education Material and Resources Final Report) commissioned by the Department of Education, Skills and Employment in 2021.
- The Australian Government could partner with states, territories, and non-government school systems and be informed by experts to support schools in the delivery of high quality, age-appropriate, evidence-based respectful relationships education. This could include consideration of resources and professional learning for educators, frontline workers, including social workers and general practitioners on online pornography integrated with respectful relationships education.
- The need for public awareness raising efforts to promote understanding of and trust in any age assurance pilot or mandate.

Consultation

A program of consultation with community, industry, and government stakeholders

eSafety conducted extensive multi-sector stakeholder consultation to inform this report. We are grateful to the organisations who participated in this process, which are listed in Appendix B.

Throughout the consultation process, stakeholders emphasised governments should regulate online content and activity in a way that promotes human rights and supports international and cross-disciplinary collaboration. Measures should be developed in consultation with the NGOs, academics, and researchers working on these issues, and consider the human behaviours, motivations, and the important roles of parents and carers, peers, schools, and other services in children's lives.

Several other government processes explored in this report also involved significant public consultation, such as the review of the Privacy Act and the consultation on the exposure draft of Trusted Digital Identity Bill 2021.

Stakeholder consultation will continue to be a crucial element of the roadmap's consideration and implementation. For many regulatory activities within eSafety's remit – such as the online industry's development of co-regulatory industry codes or eSafety's development of industry standards – stakeholder consultation is a legislative requirement.

Roadmap

Next steps

Some of the key points at which further consultation will occur include:

- Phase 2 industry codes or standards
- The development of further education and Safety by Design resources
- The review of the Online Safety Act

Appendix A:

Recommendations for the Australian Government

eSafety recommends the Australian Government

1. **Fund specialist researchers and experts in working with younger children on sensitive issues to conduct research examining:**
   - The content of online pornography that children and young people are encountering.
   - The impacts on and feelings of children and young people.
   - What children and young people are learning from online pornography.
   - Pathways into and factors that influence encounters with online pornography.
   - How emerging technologies and online environments, such as virtual/augmented/extended reality and the metaverse, change the ability to access and the nature of engagement with online pornography, and the potential impacts on children.
   - Attitudes towards and impacts of online pornography among at risk groups, especially those who are underrepresented in current research, including Aboriginal and Torres Strait Islander and culturally and linguistically diverse children and young people.
   - The experiences and impacts of online pornography on children and young people under 16, and especially under 12.
2. **Develop, implement, and evaluate a pilot before seeking to prescribe and mandate age assurance technologies for access to online pornography.**
   - eSafety recommends a trial of age assurance technologies and the use of digital tokens in the Australian context. This reflects international experience, similar State initiatives such as Service NSW's digital age verification pilot and aligns with independent technical advice.
   - While eSafety should be involved in the development, implementation, and evaluation of any such pilot, we do not presently have the resources or expertise to lead its delivery.
   - eSafety recommends the Australian Government consider the suggested arrangements on pages 22-25 and 35, including in relation to:
     - a privacy impact assessment
     - collaboration with euCONSENT
     - multiple use cases
     - user choice
     - the range of technologies
     - double-blind, tokenised approach
     - consultation
     - awareness raising
     - comprehensive and transparent evaluation
     - cross-government stewardship.

3. Fund eSafety to:

- Develop bespoke Safety by Design resources on good practice in relation to age assurance and complementary measures to create safe and age-appropriate online spaces.
- Establish an online safety tech centre which serves to support parents, carers and others to access, understand and apply safety technologies that work best for their family's circumstances as one part of a holistic approach to online safety. This centre could also support schools in relation to the use of safety technology, in partnership with state and territory governments.

4. Conduct further work to:

- Determine the extent to which the cost, availability, awareness, or any inherent practicalities associated with safety technologies such as filters and parental controls present a barrier to their uptake by Australian families.

5. Fund eSafety to:

- Review existing resources for alignment with the findings of the roadmap and background report and:
  - Work with subject matter experts and communities to develop a suite of evidence-based, age-appropriate educational resources about online pornography for children and young people from a range of backgrounds and life experiences, such as First Nations children, LGBTIQ+ children, culturally and linguistically diverse (CALD) children, children with disabilities and children who are especially at-risk.
  - Develop complementary resources for parents, carers and frontline workers to equip them to have age-appropriate conversations about online pornography and implement technological tools to prevent and mitigate harm associated with online pornography.
  - Update eSafety's Toolkit for Schools and professional development resources for educators with information about online pornography, including strategies for preventing and managing pornography-related incidents and support pathways for students and families.
- Raise awareness of any new resources among key stakeholders and relevant groups.

6. Consider the development of a mechanism for greater national coordination and collaboration of respectful relationships education

- Ensure the mechanism is consistent with the Monash University report (Respectful Relationships Education in Australia: National Stocktake and Gap Analysis of Respectful Relationships Education Material and Resources Final Report) commissioned by the Department of Education, Skills and Employment in 2021.
- The Australian Government could partner with states, territories, and non-government school systems and be informed by experts to support schools in the delivery of high quality, age-appropriate, evidence-based respectful relationships education. This could include consideration of resources and professional learning for educators, frontline workers, including social workers and general practitioners on online pornography integrated with respectful relationships education.

Appendix B:

Consultation participants

Organisations that participated in multi-sector consultation process*	
18North	IIS Partners
5Rights	It's Time We Talked
Australian Curriculum, Assessment and Reporting Authority (ACARA)	Jumio
	Mastercard
ACT Education Directorate	Meta
Association of Heads of Independent Schools of Australia (AHISA)	Microsoft
	MindGeek
Alannah and Madeline Foundation	OnlyFans
Apple	Optus
Age Verification Providers Association (AVPA)	Our Watch
	Privately
AgeChecked	Queensland Police Service
Bumble	Queensland Department of Education
Collective Shout	Reddit
Communications Alliance	The Reward Foundation
Crisp Thinking	Roblox
Digital Industry Group Inc. (DIGI)	Safecast
Digital Rights Watch	Scarlet Alliance
Discord	Snap Inc
eftpos	Spectrum Ai
Electronic Frontiers Australia	Teach Us Consent
Equifax	TikTok
Eros Association	TrustElevate
euCONSENT	Twitter
Family Zone	VerifiiD
Google	VerifyMyAge
Griffith Youth Forensic Service	Victoria Department of Education
Interactive Games and Entertainment Association (IGEA)	xHamster
	YOTI

Organisations that participated in multi-sector consultation process* (cont.)
Academics associated with the following institutions: • Aston University • Burnet Institute • London School of Economics and Political Science • Middlesex University • Queensland University of Technology • Technological University Dublin • University of New South Wales • University of Sydney • Western Sydney University
Federal Government departments and agencies consulted
Attorney-General's Department
Australian Cyber Security Centre
Australian Human Rights Commission
Australian Competition and Consumer Commission
Department of Home Affairs
Department of Infrastructure, Transport, Regional Development, Communication and the Arts
Department of Education
Department of Social Services
Digital Transformation Agency
Office of the Australian Information Commissioner
Services Australia
eSafety groups consulted
National Online Safety Education Council
Online Safety Youth Advisory Council
Trusted eSafety Providers
Other
Members of the International Working Group on Age Verification

* One organisation withdrew from consultation.

References and notes

1. A range of stakeholders, including sex workers who attended our consultation sessions as well as children and young people who participated in our focus groups, talked about the importance of language in framing discussions around pornography, as it can either contribute to, or help to mitigate, shame and stigma. Some stakeholders felt using the term 'exposure' has the potential to stigmatise online pornography as something inherently negative. The roadmap therefore focuses on children 'accessing', 'encountering', or 'viewing' pornography. We have used 'exposure' when it is necessary for accuracy, such as quoting from eSafety documents produced before our consultation period, or reflecting specific language used in a survey cited in the evidence.
2. Enex TestLab is a commercial independent testing lab with over 30 years' experience providing search and testing services for private sector and governmental bodies.
3. As of March 2023, eSafety is working to finalise the background report.
4. As explained below, the roadmap considers the broader range of age assurance technologies (such as age estimation) rather than limiting its assessment to age verification.
5. See e.g. WeProtect Global Alliance Intelligence Briefing, The role of age verification technology in tackling child sexual exploitation and abuse online, November 2022.
6. eSafety, Safety by Design Principles and Background, May 2019.
7. 5Rights Foundation, But how do they know it is a child? Age assurance in the digital world, October 2021.
8. Quadara A, El-Murr, A & Latham J, The effects of pornography on children and young people, An evidence scan, 2017, Australian Institute of Family Studies.
9. eSafety, Regulatory Posture and Regulatory Priorities 2021-22, November 2021.
10. See e.g. Ofcom, Joining forces to help protect children online, 24 March 2023.
11. C Chen, Introducing Age Verification, 21 September 2021.
12. Google, Ensuring Age Appropriate Experiences, 17 March 2022.
13. A UK-based company which provides identity and age assurance solutions, including facial age estimation.
14. Yubo, Goal: 100% Age-Verified Users on Yubo!.
15. Meta, Introducing New Ways to Verify Age on Instagram, 23 June 2022.
16. eSafety, Public perceptions of age verification for limiting access to pornography, October 2021.
17. See e.g., Digital Industry Group Inc. (DIGI) and Communications Alliance, Consolidated Industry Codes of Practice for Online Class 1 Content Community Research, September 2022 (82% of respondents said that self-declaration of age is not effective, and 59% supported stricter confirmation of age); UK Information Commissioner's Office and Ofcom, Families' attitudes towards age assurance, 11 October 2022 (most parents felt that online services should have age assurance measures).
18. Facial analysis for age assurance purposes is not the same as facial recognition for identity verification. Facial analysis estimates a person's age without identifying an individual.
19. The Privacy Act Review Report, released by the Attorney-General's Department (AGD) in February 2023, puts forward a range of proposals designed to ensure Australia's privacy framework responds to new challenges in the digital era which may assist mitigating some concerns regarding the collection and use of sensitive information. Public feedback on the Report will inform the Australian Government's next steps. The review is discussed further below.
20. Hard identifiers are verified sources of ID used to prove a user's age. This can include government-issued identity documents such as drivers' licences and passports or credit cards.
21. For example, hard identifiers are generally used to conduct pre-employment checks, purchase alcohol, enter an age-restricted venue and gain access to government services.
22. The assessment considered Publicly Available Specification (PAS) standard 1296, Institute of Electrical and Electronics Engineers (IEEE) standard IEEE Std 2089 – 2021, International Organization for Standardization (ISO) draft standard Information technology – Age assurance systems – Framework.
23. See e.g. Equifax, Submission to the inquiry into age verification for online wagering and online pornography; Yoti, Reusable age checks.
24. J Gorin, M Biéri and C Brocas, Demonstration of a privacy-preserving age verification process, 23 June 2022.
25. *Online Safety Act 2021* (Cth) Part 9.
26. *Online Safety Act 2021* (Cth) s 108.
27. *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth).
28. Electronic services where the sole or primary purpose is to enable online social interaction between two or more end-users, who can link to, or interact with, some or all other end-users and post material on the service. *Online Safety Act 2021* (Cth) s 13.

29. This includes email, instant messaging, SMS, MMS, and chat services which enable end-users to communicate with other end-users, as well as services which enable end-users to play online games with each other. *Online Safety Act 2021* (Cth) s 13A.
30. Other services which allow end-users to access material using an internet carriage service, or which deliver material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of an internet carriage service. *Online Safety Act 2021* (Cth) s 14.
31. eSafety, Industry codes.
32. eSafety's background report explores these limitations and challenges in depth. For example, it is often very difficult for researchers to recruit enough children and young people for representative studies on these topics due to necessarily strict ethical standards, the need for parental consent and current recruitment techniques. Studies submitted to eSafety in our call for evidence varied in their descriptions of pornography and of harm, how they described and captured information about access and the age of participants involved. As such, studies should be compared with care.
33. For example, through our consultations, we spoke to clinical therapists for young people who have been court-sanctioned for sexual offences. They described discussing pornography consumption with their clients as a potential factor in their behaviour on a case-by-case basis, noting it can be difficult to disentangle any potential impacts of a young person's pornography consumption from other factors that may have contributed to their harmful behaviours, such as adverse childhood experiences including maltreatment, dysfunctional families, domestic violence, sexual victimisation, or a lack of protective factors.
34. eSafety acknowledges the binary labels of 'intentional' or 'unintentional' may fail to capture the nuanced spectrum of interactions children have with online pornography and our background report explores some of these nuances, including how different ways of characterising access may stigmatise users, including children, or reduce the responsibility of online service providers. We have opted to distinguish access as intentional or unintentional (acknowledging the potential fluidity between these descriptors) and have sought to explore this distinction in a judgment-free way to explore the impact of this context on the potential risks, harms, and proportionate interventions.
35. Litsou, K., Byron, P., McKee, A. and Ingham, R., 2020. Learning from pornography: results of a mixed methods systematic review. Sex Education, 21(2), pp.236-252.
36. Throughout this paper, we use the acronym 'LGB+' to refer to our research findings relating to sexually diverse young people. We use other acronyms, such as 'LGBTIQ+' (lesbian, gay, bisexual, trans, intersex, queer, and more) when referring to other research, to accurately reflect the participants within each study.

    Our research and survey aimed to be inclusive of a diversity of cultures. However, it could not provide quantitative analysis for all groups. Our sample (n=1004) included 16–18-year-olds with disability (n=228), those who speak a language other than English (LOE) at home (n=247), those who are LGB+ young people (n=219), trans and gender-diverse participants (n=31), and First Nations participants (n=31). The numbers of First Nations participants and trans and gender-diverse participants are too small to provide for separate analysis and were not separated out of the main data collected.
37. See e.g. LaTrobe University, 2019, 'Young people, sexual literacy and sources of knowledge'. British Board of Film Classification, Young people, pornography and age verification, 2020.
38. eSafety, forthcoming.
39. Most (75%) of the 16–18-year-olds in our survey had encountered online pornography at least once.
40. No causal relationship between these factors has been established. Given the wide range of inter-connected factors which may impact a person's sexual attitudes and behaviours, it is a near-impossible task to establish causality. For example, Lim and colleagues refer to a meta-analysis of non-experimental studies considered in this research revealed a significant association between pornography (and particularly violent pornography) and attitudes supporting violence against women. However, they suggest that as men with a disposition towards violence against women may be more likely to seek out violent pornography, the association cannot be interpreted as causation. [Lim MSC, Carrottte ER, Hellard MR, 'The impact of pornography on gender-based violence, sexual health and well-being: what do we know?' *J Epidemiol Community Health*, January 2016. 70, 1 DOI: 10.1136/jech-2015-205453.]

    With that in mind, we note that harms-based regulators operating in circumstances of scientific complexity – for example, where multiple potential causes of harm are present – need not establish causation to take proportionate protective action. Instead, they may rely on an evidence base which establishes that a particular factor makes a *material contribution* to the harm, or *materially increases the risk of the harm* occurring.
41. Quadara et al. We note that beyond the 'mainstream pornography' considered by the AIFS study, there are many other forms and genres of pornography that would fall within the definition used within this report. This includes pornography in different mediums and created for different audiences and in different production contexts. Examples raised by stakeholders included ethically produced pornography, queer pornography, and feminist pornography. This is not meant to represent an exhaustive list of online pornographies, but rather to illustrate the range of content, genres and forms of online pornography children may encounter online.
42. See e.g., Vera-Gray, McGlynn, Kureshi, and Butterby, 'Sexual violence as a sexual script in mainstream online pornography.', British journal of criminology, 2021, 61(5):1243-1260. This and other research is further discussed in eSafety's background report.
43. Eros, Submission to age verification call for evidence and restricted access system call for submissions, 10 September 2021.
44. G Deegan, Grant Thornton resigns as auditor to firms owned by Pornhub operator, Irish Times, 9 February 2021.
45. P Hamilton, Pornography company records €19m profit at Irish arm, Irish Times, 3 January 2018.
46. MindGeek, MindGeek by the numbers.
47. Similarweb data, January 2023.
48. Vera-Gray, McGlynn, Kureshi, and Butterby, 'Sexual violence as a sexual script in mainstream online pornography.', British journal of criminology, 2021, 61(5):1243-1260.
49. Similarweb, Top websites ranking, March 2023.
50. Semrush data obtained February 2023.
51. Pornhub, EU Digital Services Act, 31 January 2023.
52. Similarweb data, February 2023.
53. See e.g. S Klein, Cypriot Pornographic Website Ban Confirmed, September 2022; Arcom, Access of minors to pornographic sites: Referral to the President of the Paris Judicial Court, 8 March 2022.
54. Arcom, Access of minors to pornographic sites: Referral to the President of the Paris Judicial Court, 8 March 2022.
55. U.K Children's Commissioner, 'A lot of it is actually just abuse': Young People and Pornography January 2023.
56. U.K Children's Commissioner, 'A lot of it is actually just abuse': Young People and Pornography January 2023.
57. There are several reasons for this, including that relevant studies point to an association between adult (18+) consumption of pornography and gender-based violence. See e.g. Vera-Gray, McGlynn, Kureshi, and Butterby, 'Sexual violence as a sexual script in mainstream online pornography.', British journal of criminology, 2021, 61(5):1243-1260. Further consideration of this issue and related research can be found in eSafety's background report.
58. Generative AI describes algorithms that allow the seamless creation of realistic text, code, audio, images, or videos based on simple text or other commands.
59. Immersive technology enables you to experience and interact in three-dimensions (3D) with digital content in a way that looks, sounds, and feels almost real. These technologies include augmented reality (AR), virtual reality (VR), mixed reality (MR) and wearables, such as haptics.
60. A National Consumer Protection Framework for online wagering in Australia was established in late 2019 and is coordinated by Commonwealth, state, and territory governments under the direction of the Department of Social Services (DSS). In May 2022, the Framework was amended, reducing the customer verification period from 14 days to a maximum of 72 hours. DSS is currently working with AUSTRAC towards pre-verification or immediate verification due for implementation in the latter half of 2023. DSS will undertake an evaluation of the reduced verification period six months following its implementation. As highlighted by the previous government's response to the Inquiry, the outcomes of this review should inform next steps for any age assurance regime introduced for online pornography.
61. *Online Safety Act 2021* (Cth) s 17.
62. *Online Safety Act 2021* (Cth) s 5.
63. *Online Safety Act 2021* (Cth) s 19.
64. *Online Safety Act 2021* (Cth) s 134.
65. *Online Safety Act 2021* (Cth) s 239A.
66. eSafety's Industry codes position paper contains an explanation at pages 22-24.
67. eSafety, Online Content Scheme: Regulatory Guidance, December 2021. As of 15 March 2023, eSafety has issued 20 class 1 removal notices and 4 link deletion notices under the Online Content Scheme. None of these actions relate to online pornography, as eSafety generally exercises discretion not to investigate online pornography reported to us (unless it is hosted in Australia or may cause serious harm to an individual or group) in order to focus our resources on the removal of child sexual exploitation material.
68. *Guidelines for the Classification of Films 2012* (Cth).
69. Australian Institute of Family Studies, Age of Consent Laws in Australia, May 2021.
70. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Review of the Australian classification regulation.
71. *Online Safety Act 2021* (Cth) Part 9, division 7.
72. *Online Safety Act 2021* (Cth) Part 9, division 8.
73. *Online Safety Act 2021* (Cth) s 151(1).
74. *Online Safety Act 2021* (Cth) Part 4.
75. *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth).

76. *Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth)* s 12.
77. Social media services, relevant electronic services, and designated internet services.
78. The Explanatory Statement provides, "Not all reasonable steps have to be taken by all service providers. Rather, they are intended to provide guidance to service providers."
79. eSafety, Basic Online Safety Expectations Regulatory Guidance, July 2022.
80. The eSafety Commissioner was a member of a panel of experts overseeing the user audit of myGov. The panel looked at how well myGov is performing in relation to reliability, functionality and delivering a user-friendly experience to inform future improvements.
81. For example, Services NSW recently announced a trial in partnership with Mastercard and same day delivery service Tipple to test whether users can verify they are older than 18 through a Mastercard ID exchange with the NSW digital identity system. NSW also plans to trial digital birth certificates in the coming months.
82. Australian Government, Digital Identity Functional Requirements, Trusted Digital Identity Framework Release 4.8, February 2023.
83. Attorney-General's Department, Privacy Act Review Report, February 2023, at p 9.
84. Attorney-General's Department, Privacy Act Review Report, February 2023, at p 8.
85. Attorney-General's Department, Privacy Act Review Report, February 2023, at p 10.
86. These include the Senate Standing Committee on Economics inquiry into the influence of large international digital platforms, the 2023-2030 Australian Cyber Security Strategy, the proposed National Human Rights Act, the proposed model law for facial recognition technology from the Human Technology Institute, and the ACCC's ongoing inquiry into digital platforms.
87. Business for Social Responsibility and Global Network Initiative, 'Human Rights Due Diligence Across the Technology Ecosystem', September 2022.
88. A child's personal ecosystem includes school, peers, parents, carers and families and other services such as health services, youth services, community services and more. This is not intended to be an exhaustive list of the digital ecosystem, but rather, to highlight key stakeholders with a role in minimising harm to children.
89. The background paper considers the rights of children, the rights and responsibilities of parents, carers and other users of online services, and human rights principles for businesses. As highlighted in UNICEF's 'Digital Age Assurance Tools and Children's Rights across the Globe', age assurance and other measures can have implications for a range of rights, including non-discrimination, participation, protection of identity, freedom of expression and access to information, education, privacy, and protection from violence and exploitation. Consistent with section 24 of the Online Safety Act and article 3 of the United Nations Convention on the Rights of the Child, eSafety considers the best interests of the child as the primary consideration.
90. Already, people have used generative AI and deepfakes to create pornography, including of real people. One prominent case involved a popular Twitch streamer accessing deepfakes of several female streamers. This sparked female streamers who were also victims of the same service, speaking out against people using this technology to create non-consensual intimate images. M Elias, A deepfake porn scandal has rocked the streaming community. Is Australian law on top of the issue?, The Feed, 9 February 2023.
91. A shared virtual space, which may be accessible through immersive technologies, where people can work, play or socialise together.
92. Some virtual reality (VR) applications enable users to craft sexualised environments and characters. There have also been instances reported of applications which allow users to simulate the sexual abuse of children. B Helm, Sex, lies, and video games: Inside Roblox's war on porn, Fast Company, 19 August 2020; S Pettifer, E Barrett, J Marsh, K Hill, P Turner, S Flynn, The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse, University of Manchester, 2022. Generative AI could power more realistic and customisable VR experiences, potentially increasing risks for children. More research is needed.
93. eSafety, Supervising Pre-schoolers online, Survey of 3,520 parents of children aged 2-17, July/August 2018.
94. Meta tags are small codes embedded in the page header which allow browsers, ISPs, search engines, filtering software and other tools to identify and block relevant content. The RTA label was created by the ASACP and is recognised by major filtering providers, including Microsoft. Many consultation participants from the adult industry said that they used this tag on their services.
95. Bounce rate refers to the percentage of visitors to a particular website who navigate away from the site after viewing only one page.
96. Dwell time refers to the amount of time a user spends looking at a web page before clicking back to the search results.
97. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Classification usage and attitudes, November 2022, at p 43.
98. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Classification usage and attitudes, November 2022, at p v.
99. eSafety forthcoming.
100. The Children's Commissioner for England, 'A lot of it is actually just abuse' Young people and pornography, January 2023.
101. Ofcom, Children's Online User Ages Quantitative Research Study, October 2022.
102. In a 2021 blog post, Facebook explained it looks at the age in users' public birthday messages to flag if a user might be underage.
103. Profiling involves making predictions or determinations about a user based on data collected as a user interacts with a service.
104. Tools which allow other users to report suspected underage users to the platform.
105. Apple, Expanded Protections for Children.
106. Google, Help keep your family safer online.
107. David Hurst, House of Commons Library, Online safety: Content filtering by UK Internet Service Providers (ISPs), 21 November 2014.
108. Ofcom, Children and parents: media use and attitudes report 2022 (ofcom.org.uk), 30 March 2022.
109. UNESCO, International technical guidance on sexuality education: an evidence-informed approach - UNESCO Digital Library, 2018.
110. eSafety forthcoming.
111. J Power, S Kauer, C Fisher, R Chapman-Bellamy & A Bourne, The 7th National Survey of Australian Secondary Students and Sexual Health, (ARCSHS Monograph Series No. 133). Melbourne: The Australian Research Centre in Sex, Health and Society, La Trobe University, 2022, DoI: 10.26181/21761522.
112. Australia's National Research Organisation for Women's Safety Limited (ANROWS), compiled data from Child at Risk Assessment Unit (2000) Age-appropriate sexual play and behaviour in children. Canberra: Department of Community Health; Pratt, R., Miller, R., & Boyd, C. Adolescents with sexually abusive behaviours and their families: Best interests case practice model (Specialist practice resource), 2022, Melbourne: Victoria Department of Human Services; Stathopoulos, M., Sibling sexual abuse. Melbourne: Australian Institute of Family Studies, 2012.
113. Discord, Policies Around Adult Content on Discord; Reddit, Reddit Content Policy; Twitter, Twitter's sensitive media policy | Twitter Help.
114. Instagram, Community Guidelines; Meta, Nudity and sexual activity: Publisher and Creator Guidelines; Snapchat, Sexual Content, January 2023; TikTok, Adult Nudity and sexual activities.
115. eSafety forthcoming.
116. UK Children's Commissioner, 'A lot of it is actually just abuse' Young people and pornography, January 2023.
117. Twitter, Media Policy, January 2023.
118. eSafety forthcoming.
119. Google, Filter explicit results using SafeSearch; Google, Creating a safer internet for everyone.
120. The role of app distribution services as gatekeepers to accessing apps means they can provide a meaningful safeguard to ensure that children can only access age-appropriate apps. Importantly, app distribution services can influence the perceived safety and trustworthiness of apps for children.
121. Browsers may offer safe browsing settings, parental controls, website blocking features or information to users about how to stay safe. In consultations, providers of safety tech stated that browsers should be required to support both first- and third-party extensions features which allow parents and carers to block adult sites.
122. Many of the stakeholders we consulted supported the use of device-based safety measures, such as parental controls and filters. eSafety's Gift Guide provides guidance to parents and carers and links to where they can find information about safety settings and tools on a variety of devices, including smartphones, tablets, gaming consoles, immersive technologies and more.
123. Google, Family Link FAQ.
124. Google, Age requirements on Google Accounts.
125. Apple, Creating your child's Apple ID.
126. Apple, Use parental controls on your child's iPhone, iPad and iPod touch – Apple Support (AU).
127. eSafety, Parenting and pornography, 2018.
128. eSafety forthcoming.
129. Child Family Community Australia, Age of consent laws in Australia, May 2021, Australian Institute of Family Studies, Australian Government. Child Family Community Australia, Age of consent laws in Australia, May 2021, Australian Institute of Family Studies, Australian Government.

130. See e.g. A McKee, "Healthy sexual development: A multidisciplinary framework for research," International Journal of Sexual Health, 2010, 22(1):14–19, DOI: 10.1080/19317610903393043; X Jiang, Age Verification, Porn Tube Sites and Children's Rights, 2019.

131. eSafety, Safety by Design.

132. Google, Using AI to keep Google Search safe, March 20, 2022.

133. eSafety, Parenting and Pornography, 10 December 2018.

134. eSafety forthcoming.

135. D Buckingham and S Bragg, 'Opting in to (and out of) childhood: young people, sex and the media', in Jens Qvortrup (ed) Studies in Modern Childhood, Palgrave Macmillan, London, 2005, DOI:10.1057/9780230504929_4; S Spišák, 'Everywhere They Say That It's Harmful But They Don't Say How, So I'm Asking Here: Young People, Pornography and Negotiations with Notions of Risk and Harm', 2016, 16(2) Sex Education 130-142, DOI: 10.1080/14681811.2015.1080158.

136. eSafety, Best Practice Framework for Online Safety Education, June 2020 – July 2021; United Nations Educational, Scientific and Cultural Organization (UNESCO), International Technical Guidance on Sexuality Education: An evidence-informed approach, revised edition, 2018; M Crabbe & M Flood, School-Based Education to Address Pornography's Influence on Young People: A Proposed Practice Framework, 2021.

137. See e.g. C Fisher, A Waling, L Kerr, et al, 6th National Survey of Australian Secondary Students and Sexual Health (ARCSHS Monograph No 113, 2019); P Ezer, L Kerr, C M Fisher, et al., 'School-based relationship and sexuality education: what has changed since the release of the Australian Curriculum?', 2020, 20(6):642-657; T M Jones, & L Hillier, Sexuality education school policy for Australian GLBTIQ students. Sex Education, 12(4):437–454; La Trobe SSS Health Survey released December 22, 2022.

138. eSafety forthcoming.

139. South Australian Commissioner for Children and Young People, Sex education in South Australia: what young people need to know for sexual health and safety, 2021. [The use of LGBTQA+ reflects the language used by the study, as they were unable to recruit enough Intersex participants to make findings for that group.]

140. Researchers have noted that the abusive scripts and unequal power dynamics found in mainstream, heterosexual pornography, can also shape the acts and depictions in LGBTQ+ pornography. Aggression and stereotyped gender roles and constructions of masculinity and femininity also feature in same-sex pornography videos. Seida, K. & Shor, E. (2021) Aggression and Pleasure in Opposite-Sex and Same-Sex Mainstream Online Pornography: A Comparative Content Analysis of Dyadic Scenes, The Journal of Sex Research, 58:3, 292-304, DOI: 10.1080/00224499.2019.1696275.

141. eSafety understands that the experiences of people with intellectual disability and neurodivergent people cannot be conflated. We group these two populations here based on similar experiences of discrimination in sex and relationships education, and similar needs for tailored education.

142. For example, Porn Is Not The Norm is a new initiative which aims to prevent young people with autism from being harmed by pornography through equipping them and their parents, carers, teachers and workers to understand pornography and how to safely navigate healthy and respectful relationships.

143. See eg. C Fisher, A Waling, L Kerr, et al, 6th National Survey of Australian Secondary Students and Sexual Health (ARCSHS Monograph No 113, 2019); Jones, T. M., & Hillier, L. (2012). Sexuality education school policy for Australian GLBTIQ students. Sex Education, 12(4), 437–454. La Trobe SSS Health Survey released December 22, 2022; P Ezer, L Kerr, C M Fisher, et al., 'School-based relationship and sexuality education: what has changed since the release of the Australian Curriculum?', 2020, 20(6):642.

144. M Lim, P Agius, E Carrotte, A Vella, & M Hellard, 'Young Australians' use of pornography and associations with sexual risk behaviours', Australian and New Zealand Journal of Public Health, 2017, 41(4):438-443. DOI:10.1111/17536405.12678; K Litsou, P Byron, A McKee, and R Ingham, 'Learning from pornography: results of a mixed methods systematic review.' Sex Education, 2020, 21(2):236-252, DOI:10.1080/14681811.2020.1786362.

145. See e.g. N Pfitzner, R Stewart, D Ollis, K Allen, K Fitz-Gibbon, A Flynn, 'Respectful Relationships Education in Australia: National Stocktake and Gap Analysis of Respectful Relationships Education Material and Resources Final Report', Monash University Report, 2022.

146. ACARA, Australian Curriculum – Version 9.0 endorsed, 2022; ACARA Australian Curriculum Review, 2022.

147. Australian Human Rights Commission, Keeping our children and young people safe: National survey on understanding and experiences of consent, 6 March 2022.

148. eSafety, Public perceptions of age verification for limiting access to pornography, 2021.

149. George Nott, Alcohol shopper age verification tech trials a success, The Grocer, 12 January 2023.

eSafety.gov.au