Roadmap for age verification

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

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.

Given the global nature of the internet, eSafety also acknowledges the inherent and continuing rights of indigenous people across the globe.

This report frequently refers to pornography and sexually explicit content. It also references sexual violence. Specific content warnings are also included in relevant chapters.

1800 Respect: 1800 737 732
Qlife: 1800 184 527
Lifeline: 13 11 14

Report parts

This volume of the report provides context on the origins and scope of the roadmap and eSafety's approach to developing the roadmap and the associated recommendations.

This volume of the report outlines the evidence provided to eSafety about children's access to online pornography – when and how they access it and the potential impacts associated with access. It also explores the relevant access points to online pornography within the digital ecosystem and how future technology trends may impact access and experiences.

This volume of the report outlines technology-based responses to preventing and mitigating harms to children from online pornography, including age assurance and other safety technologies. It assesses the risks and benefits of each technology, considers the necessary policy and regulatory settings and provides high level direction and considerations for industry.

This volume of the report is focused on how the technological measures discussed in Part 3 can be mandated and enforced through regulation. It also outlines the educational measures which should accompany any technological response, to provide a holistic approach to harm prevention and mitigation.

Part I – Framing the report

This volume of the report provides context on the origins and scope of the roadmap and eSafety's approach to developing the roadmap and the associated recommendations.

Table of contents

Chapter 1: The Inquiry

Key points

- On 1 June 2021, the previous Government announced its support for the recommendation of the House of Representatives Standing Committee on Social Policy and Legal Affairs that the eSafety Commissioner lead the development of a roadmap for the implementation of a regime of mandatory age verification for online pornography.
- The Committee recommended that the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, 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 ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

Inquiry and findings

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 Inquiry outlined the following terms of reference:

- the potential of age verification as a way to protect minors online.
- the requirements of Commonwealth, state and territory government laws, policies and practices (including technical and privacy requirements) that relate to and enable improved age verification requirements.
- the potential benefits of further online age verification requirements, including to protect children from potential harm, and to protect business and non-government organisations from reputation, operational and legal risks.

- the potential risks and unintended consequences in further restricting age verification requirements (including pushing adult consumers to unregulated content, privacy breaches, providing false assurances to parents and carers and freedom of expression).
- best practice age verification requirements around the world.
- barriers to achieving stronger age verification requirements.
- education and warning messages associated with age verification.
- the economic impact of placing further restrictions on age verification on business, including small business, and the potential financial and administrative burden of such changes.
- the impact of placing further restrictions on age verification on other eSafety resourcing, education and messaging, and Australia's international obligations.

The Committee received 325 submissions from a range of sectors and organisations, including adult industry associations, age verification service providers, academics and government agencies.[1] The Committee noted that many submissions and other correspondence 'express[ed] concern about the ease with which children and young people are able to access online pornography'.[2]

eSafety's submission to the Inquiry

eSafety provided a submission to the Inquiry, which is available on the Inquiry web page.[3]

In its submission, eSafety said a review is needed to:

- identify and develop the components of a digital ecosystem to support an age verification trial.
- understand the current capabilities and gaps in age verification technologies in Australia and what digital verification ecosystems could be leveraged for age verification.
- develop a proportionate and harms minimisation approach to age verification and determine what age verification and age assurance technologies or techniques are required to make sure children and young people are adequately protected.

[1] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, Parliament of Australia website, 2020. https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report

[2] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence.*

[3] eSafety Commissioner, *Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs,* November 2019. https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report

- consider developing a risk matrix that points to potential technological solutions that balances individuals' fundamental human rights in digital environments.
- liaise with other jurisdictions to ensure consistency, harmonisation, and amplification of efforts.
- develop measures for accountability and transparency over the security, safety and privacy of existing and proposed systems.

eSafety also made the following recommendations:

- Recognise age verification as one method for limiting children and young people's access to online pornography and accept it will take a combination of technological solutions to address the issue.
- Consider how to embed and deliver comprehensive and nationally coordinated respectful relationships and online safety education in the Australian Curriculum.
- Conduct further research into what constitutes effective education on the topic of online pornography, including content, pedagogy, professional learning and support for vulnerable groups.
- Recognise the need to improve standards of user safety in the technology community, as well as encourage and secure greater consistency and standardisation of user safety considerations by all players in the digital environment.

Inquiry findings

The Committee's report and recommendations, released in February 2020, supported the implementation of online age verification for online pornography in Australia.

Evidence submitted to the Inquiry revealed widespread and genuine concern about the impacts of online pornography and other online content on the welfare of children and young people. The Committee was told young people are increasingly accessing online pornography, and this access is associated with a range of harms relating to their health, education, relationships, and wellbeing.

The Committee also heard there was a wide range of sophisticated age verification services and technologies available. While the Committee recognised age verification is not a silver bullet, it concluded that it could create a significant barrier to prevent young people – particularly young children – from accessing harmful or age-restricted content.

Inquiry recommendation

The Committee recommended that the eSafety Commissioner lead the development of a roadmap to implement a regime of mandatory age verification for online pornographic material, and that this roadmap be part of a broader, holistic approach to deal with the risks and harms associated with online pornography. The Committee's report is available online.[4]

Recommendation 3

The Committee recommends that the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, 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 ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

The Committee also made the following relevant recommendations:

- The Digital Transformation Agency (DTA), in consultation with the Australian Cyber Security Centre, develop standards for online age verification for age-restricted products and services (Recommendation 1)
- The DTA extend the Digital Identity program to include an age-verification exchange for the purposes of third-party online age verification (Recommendation 2).

[4] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence*.

The Government's response to the Inquiry

On 1 June 2021, the previous Government responded to the Committee's recommendations.[5] The Government expressed support for **Recommendation 3**, stating in its response:

> 'The Government supports this recommendation. With children accessing or being exposed to sexually explicit material on a diverse range of online platforms, the Government recognises that there is no straightforward solution.
>
> The development of a comprehensive roadmap that adequately explores the complexities of regulating online pornography will require considerable amounts of research and stakeholder consultation over a 12-to-18-month period.
>
> The Office of the eSafety Commissioner (eSafety) is leading the development of this roadmap, in collaboration with community, industry, state and territory governments, and Commonwealth agencies including the Department of Infrastructure, Transport, Regional Development, and Communications (DITRDC); Department of Social Services; Department of Home Affairs; Digital Transformation Agency; and the Australian Cyber Security Centre.'
>
> The roadmap will be based on detailed research as to if and how a mandatory age verification mechanism or similar could practically be achieved in Australia. The roadmap, including a recommended way forward, will be provided to Government for consideration.'

The Government also provided support in principle for **Recommendations 1** and **2**:

> '[Subject to the findings of the work outlined above,] further technical standards-based work may be required which could include requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers. If so, the Government agrees that:
>
> the Digital Transformation Agency (DTA) is well-placed to develop any necessary technical standards; and
>
> the Australian Cyber Security Centre (ACSC) is well-placed to provide any necessary advice and support relating to the cybersecurity of IT systems.'

[5] Australian Government, *Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence*, Parliament of Australia website, 2021. https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Government_Response

Chapter 2: Scope

Key points

- This report explores if and how a mandatory age verification mechanism or similar could practically be achieved in Australia and recommends a way forward, including complementary measures for a holistic approach to address risks and harms associated with children's access to online pornography.
- This chapter outlines the scope of the report, regarding:
  - age verification or similar (i.e., age assurance)
  - complementary measures that support any technical solutions
  - online pornography
  - risks and harms relating to children's access to online pornography, framed in line with their evolving capacities, best interests and rights.
- Adult access to online pornography falls outside the scope of this report, as does access to sexualised material depicting or describing children.
- The use of age assurance for purposes beyond preventing children's access to online pornography is also outside of scope. However, other purposes are briefly discussed in the report to contextualise and situate the introduction and/or use of age assurance technologies within the broader landscape of online age-restricted goods and services.

Scope

As set out in the Committee's recommendation and the Government's response, this report explores if and how a mandatory age verification mechanism or similar could be achieved in Australia. It also recommends a way forward, including complementary measures for a holistic approach to address risks and harms associated with children's access to online pornography.

Age verification or similar mechanism

Age verification is a process that confirms a person's age with a high degree of certainty, using their identification attributes or other confirmed sources of information. It is one category of a broader set of processes known as age assurance.

Age assurance includes verification methods as well as processes that seek to establish, estimate or predict the age (or age range) of an individual with various degrees of certainty. Examples include self-reporting (i.e., stating your birth year), confirmation from another person (e.g., a parent), using biometric information (e.g., facial age estimation and voice analysis) or using behavioural or online signals (e.g., traces of digital usage or gesture patterns).

The stakeholders we consulted encouraged eSafety to consider the broader range of age assurance technologies rather than limiting our assessment to age verification. This is consistent with feedback received through the Attorney-General's Department's consultation on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021,[6] as well as the House Select Committee on Social Media and Online Safety *'Inquiry into Social Media and Online Safety'*.[7] It also reflects the wider range of technologies considered in comprehensive international reports on age assurance by the 5Rights Foundation[8] and UNICEF[9].

In line with these views and the Government's indication that eSafety should consider age verification or 'similar' mechanisms, this report considers a broader range of age assurance technologies. These technologies are assessed in chapter 8.

Importantly, eSafety notes that a person's age can be established without ascertaining their identity. However, currently, identity documents are commonly used as a means of determining a person's age offline and online. Similarly, many companies that offer age verification services also offer identity verification services. This report explores relevant intersections between age and identity; however it does not include or support identity verification as a condition for accessing online pornography.

[6] Attorney-General's Department, *Online Privacy Bill Exposure Draft: Published responses*. n.d https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/published_select_respondent

[7] Parliament of Australia, *Submissions received by the Committee: Inquiry into Social Media and Online Safety*, n.d. https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Submissions

[8] 5Rights Foundation, '*But how do they know it is a child?' Age Assurance in a Digital World*, October 2021. https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html

[9] UNICEF, *Digital Age Assurance Tools and Children's Rights Online across the Globe: A discussion paper*. April 2021.

Complementary measures

The Government's response to the Committee's report stated[10]:

> 'While there are no simple solutions to any online safety issue, technologies, such as age verification, age assurance and age prediction, are developing at pace. If used in conjunction with filtering and other proactive user safety settings, they can play a role in limiting exposure to harmful content for children.
>
> The Government also recognises that technological solutions alone will not stop all children from accessing online pornography or other age-inappropriate services. A multifaceted approach that includes parental engagement and education is vital to reduce the adverse effects of online pornography and other harmful content. Online safety requires long-term, sustained social and cultural change, through the coordinated efforts of the global community, and greater collaboration and consultation between industry, government and the general public.'

The Government supported the Committee's recommendation that eSafety examine complementary measures for a holistic approach to address the risks and harms associated with children's access to online pornography.

This report considers the important role that other technical measures can play to reduce harmful or unwanted access to online pornography. This includes parental controls, filters, content detection and moderation technologies and tools and settings that individuals or communities can use to reduce their own or others' contact with online pornography. More information can be found in chapters 11 and 12.

The report also considers vital non-technical measures, particularly education and awareness raising about online pornography, safety tech, sex education, consent and respectful relationships. This was supported by nearly all stakeholder groups consulted. The importance of education for children, young people and the adults who support is explored in chapter 13.

In addition, the report discusses the important role that members of the broader digital ecosystem and community can play to address the issue in part 3 of the report.

[10] Australian Government, *Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence*.

Online pornography

The way the law currently defines and applies to online pornography is discussed in chapter 14.

For purposes of this report, **online pornography** is online material that contains sexually explicit descriptions or displays that are intended to create sexual excitement, including sexual intercourse or other sexual activity.

eSafety acknowledges that this is a broad definition of pornography which will encompass a large and diverse scope of content and that defining pornography is an existing challenge across research literature. Starting with a broad definition of pornography has allowed eSafety to explore a range of studies and examine children's access to sexually explicit material in many contexts (such as both commercially available and non-commercial content).

eSafety does not suggest that any legislation or regulation should adopt this definition.

The children and young people we spoke to in focus groups conceived of 'online pornography' as encapsulating a wide range of content and activity. This included sexualised images, videos, messages, pop-ups, spam, and potential scams, as well as both the consensual and non-consensual sharing of nude or intimate images. They did not differentiate between content and activity involving those under the age of 18 (which could be classified as child sexual exploitation) versus content and activity involving adults. Further information about our research with children and young people can be found in chapters 3, 5 and 13.

Consistent with the Inquiry, the focus of this report is online pornography depicting or describing adults engaged in sexual behaviour, and primarily on content provided for a commercial purpose. However, where potential measures to prevent children's access to this type of adult material may also address broader online safety issues – such as grooming, child sexual exploitation or image-based abuse – we have sought to identify those benefits as well.

Risks and harms

In accordance with eSafety's regulatory posture and priorities, eSafety takes a 'risks- and harms-based approach to our work' and aims to 'prevent and remedy harm, enhance transparency and accountability, and examine the effectiveness and impact of what services are doing to keep users safer online'.[11] This report applies the same approach, consistent with the Committee's recommendation.

Consultation stakeholders emphasised the importance of closely examining the evidence base, noting that some research relies on potentially biased notions of what constitutes harm. Some

[11] eSafety Commissioner, *Regulatory Posture and Priorities (2021-22),* November 2021. https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes

research findings and participant insights outlined various types of online pornography – and contexts for accessing online pornography (e.g., viewing by older teens) – which may not result in harm. This issue is explored further in chapter 5.

Children's access

This report explores options to prevent and mitigate harms to children from accessing online pornography. It seeks to do so in a way that reflects children's evolving capacities and respects and upholds their best interests and rights. A discussion of rights can be found in chapter 4.

Adult access to online pornography falls outside the scope of this report. However, eSafety notes the interrelationship between children's access and adults' access, including that children's access to pornography will influence their engagement with pornography as an adult and that the pornography available for adults is frequently accessed by children. The intersection between children's and adults' access to online pornography is explored in chapters 5 and 7.

This roadmap in context

Efforts to regulate access to online pornography sit at the intersection of many different issues, including fundamental rights to safety, privacy, cultural life, work, information, expression and non-discrimination. Proposals for law and policy reform in this space – and the public's reaction to those proposals – are inextricably linked to these issues and affected by the wider socio-political and historical context. While this report cannot canvas all related matters, it seeks to acknowledge stakeholder concerns regarding the relationships between pornography and regulation and the sexualisation of children, objectification of women and girls, marginalisation of the LGBTIQ+ community, infringements on the rights of sex workers to operate safely and lawfully (issues raised during the roadmap consultations).

Historical context

Debates on the impact of pornography have a long history in feminist activism and academia.[12] These debates, especially those that occurred throughout the 1970s and 1980s in the United States, are often characterised as taking place between feminists critical of pornography, 'anti-porn' feminists, and more liberal 'sex positive' feminists. Lesbian activists and academics were at the forefront of both sides in these debates.

[12] N D Hunter, 2006. *Contextualizing the sexuality debates: A chronology 1966–2005*. In L Duggan and N D Hunter, *Sex Wars: sexual dissent and political culture,* (pp. 15-28). Routledge, London, 2006.

The feminist critique of pornography was largely based on the harm that pornography poses to women through its production and use.[13] The countermovement rejected state regulation of sexual expression and argued for the liberating possibilities of women's autonomous pursuit of sexual pleasure. Both sides of the debate were multivocal, nuanced and shared a foundation in critiques of patriarchal power. The tensions between differing feminist approaches to commercialised sexuality continue to be reflected in current public debates.[14]

The report necessarily focuses on children's access to online pornography, however the ability of digital products, platforms and services to understand the age of their users is essential to keeping them safe from a much wider spectrum of risks and harms.

eSafety recognises the applicability and importance of age assurance to a wider array of online safety issues within eSafety's existing workstreams and Australia's current online safety regulatory framework. This includes eSafety's Safety by Design initiative and the *Online Safety (Basic Online Safety Expectations) Determination 2022.* These are further detailed in chapter 12 and 14.

The extent to which age assurance policies and practices are currently being enforced was also recently considered by the House Select Committee on Social Media and Online Safety.[15]

Assessing individuals' age is also crucial for purposes of protecting their online privacy and making sure they have the capacity to provide consent to services collecting and using their data. This has been considered within Australia[16] and around the world, most notably in the United Kingdom Information Commissioner's Age Appropriate Design Code[17], discussed in chapter 10.

This report centred on the use of age assurance to reduce children's access to online pornography, but also considers synergies with other public policy issues. As discussed in chapters 9 and 10, a coordinated approach to regulating the online environment within and across governments is important to reduce inconsistency and confusion and to increase compliance and efficacy. eSafety endeavours for this report and its findings to inform future online harms initiatives undertaken internationally.

[13] See e.g. *C MacKinnon and A Dworkin, In harm's way: The pornography civil rights hearings*, Harvard University Press, Cambridge, Massachusetts, 1997.

[14] See e.g. *The* New York Times, I Still Believe in the Power of Sexual Freedom, August 2022. https://www.nytimes.com/2022/08/16/opinion/sex-women-feminism-rules.html

[15] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence.*

[16] Attorney-General's Department, *Online Privacy Bill Exposure Draft*. 25 October 2021. https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/

[17] United Kingdom Information Commissioner's Office, *Introduction to the Age appropriate design code,* ICO website, n.d. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code

Chapter 3: Methodology

Key points

- The evidence base for this report includes:
  - Submissions to eSafety's call for evidence, other relevant consultation processes and related government inquiries.
  - Desktop research and direct quantitative and qualitative research conducted by eSafety with young people and adults.
  - Sector-specific consultation meetings and roundtables eSafety convened with domestic and international experts from a variety of disciplines, as well as an independently facilitated cross-sector workshop.
  - Consultation with teams across eSafety, with the eSafety Youth Council and with agencies and departments across government.
  - An independent assessment of a range of age assurance and safety technologies conducted by Enex TestLab.
- Consistent with stakeholder guidance, eSafety has assessed and prioritised evidence based on its relevance and quality.

Overview

This chapter outlines the formation of the evidence base for this report, including eSafety's processes for evidence gathering, research and consultation.

eSafety started by reviewing the Committee's findings based on submissions, evidence, and testimony to the Inquiry. Evidence submitted to the Inquiry reflected a broad range of views and conflicting findings within the literature. So, eSafety developed a framework to evaluate the evidence put before it, including the quality of studies and their relevance to the current Australian context.

eSafety also considered submissions made to other relevant government processes, such as the Restricted Access Systems consultation[18] and the Parliamentary Inquiry into social media and online safety.[19] We found that while there is a substantial amount of evidence and investigation into the issue of children and young people's access to online pornography, some significant gaps remain.

eSafety conducted an extensive consultation process to gather insights from a wide range of stakeholders and to explore the issue holistically. The goal was not to establish a consensus view, but rather to conduct a nuanced exploration of interrelated issues which impact this work. There was significant disagreement among stakeholder groups about the extent and type of harm associated with children's access to online pornography, as well as the best ways to address this issue. However, there were also some themes which were common among most stakeholder groups. These themes have been distilled into six principles which have guided this report.

eSafety also procured independent testing to inform its understanding of the current maturity of the age assurance and safety technology market, and to assess these technologies against a series of criteria we developed based on our consultations and review of the literature. The specific methodology for that process is outlined separately in chapter 8.

In addition, eSafety drew on its internal expertise across various teams, including those specialising in education, law and regulation, research and evaluation, as well as those working to empower children and young people, diverse communities, and women. This included drawing on analysis from the eSafety investigations branch about recent public complaints received in relation to online pornography.

[18] eSafety, *Restricted Access System*, eSafety website, n.d. https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system

[19] Parliament of Australia, *Submissions received by the Committee: Inquiry into Social Media and Online Safety*.

To make sure the report reflects the broader work occurring across government which relates to minimising harm to children associated with online pornography, eSafety consulted with a range of government agencies and departments.

The purpose of this report is to identify and mitigate potential harms to children in a way that promotes and respects their rights and best interests. To that end, eSafety conducted quantitative and qualitative direct (primary) research with young people aged 16-18 and sought input from the eSafety Youth Council (whose members are aged 13-24) to make sure this report has been informed by the views and insights of children and young people.

Call for evidence submissions and desktop research

eSafety's approach to assessing the submissions and conducting supplementary desktop research aimed to explore the following questions:

Foundational research questions

- What is the nature of access to pornography by Australian children?
- What harms are associated with children's access to online pornography?
- What research is available on the effectiveness of current and proposed legislative and regulatory interventions for children's access to online pornography?
- What research is available on the effectiveness of current and proposed education about sex, consent and pornography literacy?
- What research is available on the effectiveness of current and proposed age assurance or age verification measures?

Call for evidence

eSafety issued a call for evidence on 16 August 2021. We requested insights into effective age verification techniques, as well as the impact of online pornography on children and proven methods of educating young people about both respectful and harmful sexual behaviours. eSafety also requested sector-specific evidence from:

- age verification, age assurance or third-party online identification providers
- digital environments, services and platforms
- the adult industry
- academia

- not-for-profits
- civil society.

eSafety received 33 submissions in response to the call for evidence. Common themes from submissions included the following:

- Technological measures to restrict children's access to online pornography should be proportionate to risk and harm and should not be overly prescriptive. Both platforms and users should have the ability to choose appropriate technology for their circumstances.
- Age assurance and other safety technology should be data minimising and subject to clear and transparent standards and technical requirements. Privacy and cybersecurity risks were identified as key considerations.
- There are varied research findings about the impacts of pornography on children and young people. Pornography has been associated with influencing sexual expectations and behaviours and negatively impacting understanding and practices relating to consent. It has also been associated with helping young people learn the mechanisms of sex and explore their sexual identities in an empowering way. Negative impacts are mostly associated with accidentally encountering pornography and access to violent or extreme pornography. However, not all young people are negatively impacted.
- Educating young people on healthy sexual relationships, behaviours and sexuality is important. Parents and carers, teachers, and young people should have access to more guidance and information on sex, respectful relationships and online pornography.
- The impact of age assurance measures on the domestic adult industry should be considered. This includes the regulatory cost and burden for smaller producers, the potential impact on competition, and the extent to which compliance may lead to online services censoring or de-platforming sex workers.
- There are existing initiatives in place from the adult industry and the tech industry to age restrict certain content. This includes meta-tagging and filters which block sites using those tags, requiring payment for content, and other content moderation strategies.
- A range of age assurance technologies were suggested by stakeholders all of which presented risks alongside the benefits. These include risks to privacy, barriers to inclusion and digital participation, bias in design or data, and concerns about accuracy and efficacy.

Submissions to the call for evidence submissions referred over 250 peer-reviewed academic journal articles, grey literature[20], policy papers and other relevant materials for eSafety's consideration.

In subsequent consultations, academic stakeholders told us that not all evidence should be given the same weighting, pointing out that some studies may be older, less robust, not as applicable to the Australian context or based on biased notions of what constitutes harm. Therefore, in the process of preparing this report and its recommendations, eSafety's research and evaluation team assessed the submissions and evidence provided to the call for evidence based on quality and relevance.

The evaluation criteria can be found in **Appendix 1** and was developed based on literature that detailed the key qualities of robust quantitative and qualitative research. The criteria were tested using a random selection of sources cited in submissions and then adapted to ensure it was fit for purpose. The criteria development was led by one researcher and was subject to critical review and discussion from three other members of the research team during the development and testing process.

Evidence evaluation was primarily conducted by two research team members with assistance by a third. Some sources were evaluated by multiple researchers, and additional team members provided consultation and review of evaluated sources to ensure consistency and mitigate bias.

This assessment impacted the weighting given to the evidence which is throughout this report. Academic studies submitted directly to the call for evidence and rated highly against the above criteria have been prioritised and given stronger weighting in this report.

The list of topics on which evidence was requested from each sector and a thematic summary of responses is included at **Appendix 2.**

Other eSafety consultations and processes

Restricted Access System Declaration consultation

The call for evidence was conducted alongside a separate but related consultation process on Restricted Access Systems (RAS).[21] The Online Safety Act 2021 (Cth) ('the Act') defines a RAS as an access-control system with the objective of protecting children from exposure to material that is unsuitable for them.[22] Specifically, it applies to material provided from Australia that has been or is likely to be classified R18+ or Category 1 Restricted ('Restricted Material') under the

[20] Research material which is published outside of commercial or traditional academic journals and can include reports and working papers.
[21] eSafety, *Restricted Access System.*
[22] Online Safety Act 2021 (Cth), s 108. https://www.legislation.gov.au/Details/C2021A00076

National Classification Code. eSafety was required to have the Restricted Access System Declaration in place from January 2022 setting out the requirements for a RAS.[23] More information about the RAS Declaration and classification system is in chapter 14.

eSafety ran two consultation processes in 2021 to help develop the *Restricted Access Systems Declaration 2022*. The first consultation phase involved a public call for submissions in relation to several questions in a discussion paper published in August 2021.[24] The second phase, in November 2021, sought feedback on the draft instrument and explanatory statement.[25]

Relevant submissions to the RAS consultation process were considered in developing this report and its recommendations.

Online Safety Consultative Working Group Expert Panel Report

In 2016, the Australian Government tasked the eSafety Commissioner with forming an Expert Panel in response to the Harm being done to Australian children through access to pornography on the Internet report.[26]

The Online Safety Consultative Working Group Expert Panel prepared a report and recommendations, which were presented to Government in 2017.[27] eSafety has drawn on its insights for this report.

Consultation with First Nations communities on online safety issues

In 2022, representatives from eSafety travelled to several regional and remote First Nations communities to consult with community members aged 10 to 70 on a range of online safety issues. In many 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. eSafety has also drawn on those conversations for this report.

[23] Online Safety Act 2021 (Cth) s 108(5).

[24] eSafety, *Restricted Access System Online Safety Act 2021: Discussion Paper,* August 2021. https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system#downloads

[25] eSafety, *Online Safety (Restricted Access Systems) Declaration 2021*. August 2021. https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system#downloads

[26] Parliament of Australia, Senate Environment and Communications References Committee, *Harm being done to Australian children through access to pornography on the internet*, Parliament House, Canberra, 2016.

[27] The Expert Panel comprised of the members of the 'Contact and Content' sub-committee of the Online Safety Consultative Working Group. The panel represented a range of fields and provided information and insights both specialised and specific to their areas of expertise.

Desktop research

Rapid literature review

In 2021 eSafety surveyed available literature to inform anticipated primary research undertakings.

In August 2022, eSafety conducted an updated rapid literature review to capture additional material that may have been published since the previous review or may not have been captured. The review focused on literature which offered insights from both academic and grey literature published in English within the past four years (2018-2022) and within similar jurisdictions[28]. The review found 45 grey literature papers and 32 peer reviewed and/or conference papers.

Relevant government inquiries or consultation processes

Several recent government inquiries or other public consultations have considered issues relevant to this report, and submissions to those processes have been considered where relevant. In addition to the Inquiry which gave rise to this report, this includes:

- the House Select Committee on Social Media and Online Safety *Inquiry into Social Media and Online Safety.*[29]
- the Attorney-General's Department's consultation on the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021.*[30]
- Industry groups' public consultation (as well as related research) on draft industry codes to address the detection and removal of illegal and restricted online content.[31]

Transparency Reports and other sources

eSafety also considered various reports by international organisations and trust and safety reports produced by digital platforms and services when developing the roadmap and this background report. The extensive list of sources is outlined in our references.

[28] Literature from before 2018 was included if it was highly cited or considered seminal.
[29] Parliament of Australia, *Submissions received by the Committee: Inquiry into Social Media and Online Safety*,
[30] Attorney-General's Department, *Online Privacy Bill Exposure Draft: Published responses*.
[31] Online Safety Industry Steering Group, *Online Safety Codes* n.d. https://onlinesafety.org.au/

Primary research

Public perceptions of age verification for limiting access to pornography

In March and April 2021, eSafety designed and conducted an online survey of 1,200 adults living in Australia, to better understand people's awareness and acceptance of age verification technologies for preventing children's access to online pornography.

The survey explored:

- adult internet usage, frequency and habits
- the general community's awareness, understanding and expectations of age verification technologies.
- perceived benefits and barriers to age verification solutions (which verify a minimum age to access online pornography)
- expectations if the Australian government were to implement such measures.

A short peer review consultation process was undertaken to explore wording, comprehension and understanding of the proposed survey items (including any gaps in the questioning against the research objectives).

A non-probability (or opt in) online panel from I-Link Research Solutions was used to access a sample of the Australian general community of adults.[32] Quotas were put in place to reflect age, gender and location (state/territory) data from the Australian Bureau of Statistics (ABS) 2016 census data. A demographic breakdown of participants is in **Appendix 3**.

The final approved questionnaire was provided to i-Link for programming and distribution to their panel members. Data collection was conducted between 29 March and 13 April 2021. The survey was about 12 minutes long on average. A total of 1,200 surveys were completed.

A weight was calculated for each survey respondent. The data was weighted to ABS data for age, gender and location (state/territory). Weighting made no significant differences to the results at the total level, but it was applied in analysis for consistency across sub-group and total results reported.

A summary of the survey findings was published on eSafety's website.[33]

[32] The online panel was a non-generalisable community sample with limited options for statistical testing. Although online panel providers make efforts at recruiting a broad population, there is research that indicates online panel samples may under-represent some subgroups compared with others.

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

Young people's experience with and perceptions of online pornography

Following the call for evidence, initial consultation sessions and desktop research, it became clear that much of the research on children's and young people's perspectives on online pornography has been conducted internationally. There is limited recent evidence available on the perspectives and attitudes of Australian children and young people to online pornography and its impact on their development, expectations of intimate relationship and sexual behaviours.

There is also little recent evidence on young Australians' lived experiences, including those of Aboriginal and Torres Strait Islander children and young people, LGBTIQ+ children and young people, those with disability, and those of culturally and linguistically diverse backgrounds.

Research is also limited – domestically and internationally – on children's and young people's views about necessary educational tools and resources (e.g., for young people, parents and teachers), or their attitudes to age verification or other technological solutions that seek to restrict underage access to online pornography.

eSafety's research program sought to address these gaps and contribute to the body of evidence on these issues by examining the perspectives of young people towards online pornography, its potential harms, and the technical, educational and other ways to prevent and mitigate such harms.

In September 2022, eSafety conducted quantitative and qualitative research with participants aged 16-18. This piece of research explored:

- participants' lived experience in relation to their encounters with and ideas about online pornography
- what support they want to receive about navigating online pornography
- their views on age-based restrictions of online pornography and on age verification technology

The research was conducted in two phases – an online survey followed by online focus groups. The research was submitted as part of the Human Research Ethics Committee (HREC) approval process with ethics approval obtained from Bellberry Ethics Committee on 26 August 2022, ID 22CeSC117. eSafety collaborated with Professor Bronwyn Carlson and Madi Day of Macquarie University's Department of Indigenous Studies to review the methodology and instruments for cultural safety and to make sure questions were worded in a culturally sensitive manner.

Online survey

eSafety surveyed 1,004 young people aged between 16-18.

The survey was conducted Australia wide, with participants from all states and territories and both regional and metropolitan locations. Participants included those attending formal education, including high school, university, vocational training, as well as those working or seeking employment.

Participants also included young people from groups identified as being most at risk of online harm: Aboriginal and Torres Strait Islander young people, LGBTIQ+ young people, those with disability, and those of culturally and linguistically diverse (CALD) backgrounds. A demographic breakdown of participants is in **Appendix 4.**

Survey participants were recruited directly via an online research panel from Octopus Group, and asked for their consent directly, as 'mature minors.' They were not recruited through their parents and were not required to gain parental consent to participate. This was done to mitigate the risk that young people in out-of-home care, those who are not close with their parents, carers or guardians, and those who do not feel comfortable discussing subjects like online pornography with their parents, would be excluded from the study.

Participants completed a questionnaire of at least 15 minutes, which involved 40 close-ended questions. Octopus Group hosted the survey, collected and cleaned the survey data, and provided eSafety with raw data as well as descriptive analysis. eSafety checked and analysed the data using SPSS Statistics software.[34]

Online focus groups

Thirty-two young people participated in six one-hour online text-based focus groups. Participants were recruited from survey participants and through Q&A, a market recruiter company. As with the survey, participants were recruited directly, instead of through parents or carers. Informed consent to take part was sought directly from participants. Involvement in the focus groups was pseudo-anonymous.

Participants included young people with a range of genders and sexualities. The focus groups were made up of 12 sixteen-year-olds, 11 seventeen-year-olds and 10 eighteen-year-olds. There were 15 women, 11 men, four non-binary young people, one trans man and one demiboy in the focus groups. Nineteen focus group participants identified as straight, one as gay, three as queer, five as bisexual, one as pansexual, one as asexual, one as demisexual panromantic and one as questioning. In this report, we attribute quotes from focus group participants based on age only, to preserve the anonymity of participants.

[34] SPSS Statistics is a statistical software suite developed by IBM.

The aim of the focus groups was to add depth and nuance to the survey findings and draw out young people's experiences and views in their own words. Based on participants' expressed preferences, one focus group consisted of LGBTQA+ young people only, and one consisted of heterosexual young men only. Four focus groups were not categorised according to gender identity or sexuality. The focus group composition can be found in **Appendix 4**.

Qualitative analysis tool Condens was used to review and analyse focus group transcripts, following Braun and Clarke's (2019) method for thematic analysis.[35] Quotes from focus group participants can be found throughout this report and have been edited for spelling and grammar.

Other relevant research commissioned or produced by eSafety

While not produced for this report, the following research commissioned or produced by eSafety informed the development of this report:

- The research led by the Young and Resilient Research Centre at Western Sydney University – Consultations with young people to inform eSafety Commissioner's engagement strategy for young people. In 2021, Western Sydney University ran a Living Lab process to help develop eSafety's Engagement Strategy for Young People. The process used youth-centred, participatory co-research and co-design methods to develop recommendations for, among other things, eSafety's engagement with children and young people.
- Mind the Gap – Parental awareness of children's exposure to risks online. This research surveyed 3,500 young people aged 8 to 17 and their parents. The research methodology report is available on eSafety's website.
- Parenting and pornography**:** findings from Australia, New Zealand and the United Kingdom. This research from 2018, conducted in partnership with Netsafe, UK Safer Internet Centre and Plymouth University, surveyed parents to understand parents' attitudes and views about their children's experiences with online pornography.

Technology testing

eSafety engaged Enex TestLab to test a range of age assurance and safety technologies against a series of criteria, including feasibility, sensitivity of data, security and integrity, barriers to inclusion, potential for bias and accessibility. The criteria were developed by eSafety and

[35] V Braun, V Clarke, *Reflecting on reflexive thematic analysis*. Qualitative research in sport, exercise and health, 11(4), 2019 pp.589-597.

informed by insights and issues raised during the consultations process, as well as by existing literature on age assurance and relevant technologies.[36]

Wherever possible, Enex TestLab applied objective assessments and measures. In some instances, this was not feasible, so it relied on subjective assessment and observation. The experiment design and results are discussed further in chapter 8**.**

Consultation

eSafety held 28 consultation meetings with 65 stakeholders and stakeholder organisations across a range of sectors.

Date	Stakeholder group
November 2021	• Law enforcement • International adult industry • Domestic adult industry • Domestic academics • International academics • International children’s wellbeing and rights advocates • Domestic children’s wellbeing and rights advocates • International age assurance and safety technology providers • Domestic age assurance and safety technology providers
January 2022	• Domestic academics
February 2022	• Domestic children’s wellbeing and rights advocates • Domestic adult industry (session 2)
March 2022	• State education departments and education authorities • Digital rights and standards advocates
April 2022	• Business and financial services • Digital platforms and services
May 2022	• Additional digital platforms and services

[36] Berkman Centre for Internet & Society, *Enhancing Child Safety & Online Technologies: Final Report of the internet Safety Technical Task Force,* December 2008. https://cyber.harvard.edu/pubrelease/isttf/; UNICEF, *Digital Age Assurance Tools and Children’s Rights Online across the Globe: A Discussion paper*, April 2021; 5Rights Foundation, *‘But how do they know it is a child?’ Age Assurance in the Digital World*; UK information Commissioner’s Office, *Information Commissioner’s opinion: Age Assurance for the Children’s Code*, October 2021. https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf; Center for Democracy and Technology, *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis,* May 2021. https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/; S Van der Hof and S Ouburg, *Methods for Obtaining Parental Consent and Maintaining Children Rights,* euCONSENT, September 2021. https://euconsent.eu/download/methods-for-obtaining-parental-consent-and-maintaining-children-rights/; S Smirnova, S Livingstone and M Stoilova, *Understanding of user needs and problems: a rapid evidence review of age assurance and parental controls*, euCONSENT, September 2021. https://euconsent.eu/download/understanding-of-user-needs-and-problems-a-rapid-evidence-review-of-age-assurance-and-parental-controls/; Australian Government, *Trusted Digital Identity Framework policy documents.* n.d. https://www.digitalidentity.gov.au/tdifdocs

June 2022	• Domestic prevention of gender-based violence not-for-profit organisation
July 2022	• Privacy advocates

The consultation sessions were held under the Chatham House rule,[37] and high-level and anonymised summaries of each discussion have been published on eSafety's website. The consultation summaries are available at **Appendix 5** and a list of consulted stakeholders and organisations is at **Appendix 6.**

eSafety also provided a survey link to interested parties who did not participate in consultation meetings. This included individuals and organisations who indicated their interest in participating in the consultation process by registering their interest on eSafety's website. Three responses were received and were considered alongside the evidence presented during consultations.

Cross-sector workshop

Following the sector-specific focus groups, eSafety held an independently facilitated workshop in July 2022 which brought together stakeholders from different sectors. This provided an opportunity for a multi-disciplinary and nuanced discussion of the issues raised in sector-specific consultations.

The objectives of the workshop were to:

- Bring stakeholders together to make sure previously expressed views have been properly captured and to enable all groups to build an understanding of the full range of competing factors that must be balanced in developing the roadmap.
- Define principles that would assist in shaping the direction of the report and its recommendations, balancing areas of consensus and disagreement.
- Consider and identify proportionate and feasible measures for reducing the risks and harms of underage access to online pornography.
- Deliberate the roles and responsibilities of government, industry, family and others.

eSafety asked participants to respond to six draft principles developed to guide the drafting of the report, and to consider the implementation of different potential measures in the context of three case studies.

eSafety used these discussions to guide consideration and assessment of the available measures within the roadmap. eSafety also considered the workshop feedback to further refine

[37] Under the Chatham House Rule, anyone who comes to a meeting is free to use information from the discussion but is not allowed to reveal who made any particular comment. It is designed to increase openness of discussion.

the guiding principles framing this report. An anonymised summary of the workshop discussion was published on eSafety's website in January 2023 and is available at **Appendix 7.**

eSafety Youth Council

The eSafety Youth Council (council) was appointed in April 2022. It was set up to provide young people with a national voice on online safety policy. The 25 council members are aged 13 to 24 years and are from a diverse range of experiences, genders, cultural and linguistic backgrounds, and locations.

Between December 2022 and February 2023, eSafety consulted the council, who provided their views on different types of age verification and age assurance methods. This consultation informed the assessment of the age verification market and the suitability of tech options outlined in chapters 8, 11 and 12.

Council members held a discussion on the roadmap during their December 2022 meeting and a follow up discussion continued using a dedicated online forum. Noting that the council members ranged in age from 13-24, the general group discussion did not focus on age verification and age assurance in relation to online pornography. Instead, it discussed the technology in the context of general online safety and included consideration of age assurance for social media sites to prevent older users from contacting younger ones. We asked council members to consider different types of technology used to verify or estimate age online and asked for their views on the benefits and risks.

A separate online discussion was held with young adult council members (18-24) in February 2023 to discuss age verification and age assurance in the specific context of online pornography.

Trusted eSafety Providers

eSafety plays a role in enhancing and promoting the development of the external education provider sector through the Trusted eSafety Provider Program.[38] eSafety works with its endorsed providers through a community of practice to provide professional learning and to share research and insights on emerging online safety issues.

eSafety briefed providers on the roadmap at their December 2022 community of practice meeting. This briefing covered relevant themes arising from consultation meetings and sought provider reflections on these initial findings based on their experience delivering online safety education.

[38] eSafety, *Trusted eSafety Providers*, n.d. https://www.esafety.gov.au/educators/trusted-providers

Cross-government consultation

The government response to the Inquiry indicated that to develop the roadmap, eSafety would collaborate with state and territory governments, and Commonwealth agencies including the (then) Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), the Department of Social Services (DSS), Department of Home Affairs (DHA), the Digital Transformation Agency (DTA), and the Australian Cyber Security Centre (ACSC).

Recognising the range of considerations within this report and the need to take a holistic approach, eSafety consulted with several other state and territory and Commonwealth agencies and departments. This included discussions with members of the new National Online Safety Education Council, an eSafety-led forum for key school education stakeholders to address shared online safety challenges and promote best practice approaches to online safety education across Australian schools.[39]

eSafety has also engaged with foreign governments to discuss policy and regulatory settings, legislation, enforcement and compliance. A comprehensive list of consulted agencies and departments is included in our stakeholder list at **Appendix 6.**

Guiding principles

Following the first two rounds of stakeholder consultation, eSafety distilled the emerging common themes into six draft guiding principles. These were tested and refined in a cross-sector workshop. Our principles intend to be complementary and compatible with other relevant domestic and international published principles.

Take a proportionate approach based on risk and harm

eSafety will draw on a robust, diverse and interdisciplinary evidence base to understand the nature of the risks and harms – and the areas where there is greater or lesser evidence and agreement. Proposed measures will be reasonable and targeted to the risk of harm across different contexts. The risks and consequences of proposed interventions will be considered and balanced.

Respect and promote human rights.

Making the online world a safer, more inclusive, and accessible space is ultimately about fulfilling the human rights of those who inhabit it. The rights of all relevant stakeholders will be considered, with the best interests of the child as the paramount consideration, informed by

[39] eSafety, *Educators commit to closer cooperation for online safety*, 13 December 2022. https://www.esafety.gov.au/newsroom/media-releases/educators-commit-closer-cooperation-for-online-safety-0

the full range of rights articulated in the United Nations Convention on the Rights of the Child[40] and General Comment 25 on children's rights in relation to the digital environment.[41]

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

Reducing the risks associated with children's access to online pornography requires a whole-of-community approach which considers the different situations and reasons children encounter or seek out this material. eSafety will consider how government, the online industry, safety technology providers, the adult industry, educators and frontline workers, parents and carers and children themselves can contribute to reducing harm, and how their roles may shift in different contexts and as children mature. It will also consider how to equip those who may need extra help, and how to support children who may lack access to relevant education or to safe and supportive school and family environments.

Ensure any technical measures are data-minimising and privacy preserving.

Safety measures will not be effective unless they are private, secure and trustworthy. eSafety will consider the sensitivity and protection of the data required by different age assurance technologies, the placement of those technologies within the digital stack, the standards by which the technologies would need to be accredited and audited, and the oversight and redress mechanisms which would need to be in place to uphold privacy and ensure accountability.

Consider the broader domestic and international regulatory context.

Both the domestic and international regulatory landscapes are highly dynamic, and influenced by a range of social, cultural and *political* factors. eSafety will consider age assurance requirements and other related developments which are either in place or being considered within Australia and overseas, and the potential for regulatory burden, particularly for local businesses. Proposed measures will promote collaboration and interoperability.

Consider what is feasible now and anticipate future environments.

Measures should not be 'set and forget', especially for privacy and security requirements. While there is a range of technical options currently available and in use to reduce children's access to online pornography, they are associated with different levels of assurance, accuracy, equity and data collection. Proposed measures will reflect the feasibility and limitations of current technology, encourage ongoing innovation and improvement, and be adaptive and flexible to

[40] United Nations, *Convention on the Rights of the Child*, 1990. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[41] United Nations, *General comment No 25 (2021) on children's rights in relation to the digital environment*, 2 March 2021. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

emerging online environments that include new users, behaviours, and tools.

A note on the importance of language

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. This report 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.

There were differing views about distinguishing ‘accidental’ from ‘intentional’ access to online pornography. Some stakeholders felt this could be interpreted as placing blame on children who seek out material. Others felt it was not a meaningful distinction for purposes of identifying possible harm. However, the majority view was that understanding the context in which children encounter pornography unexpectedly – as well as the different reasons why children may seek out this material – is key to establishing potential risks, harms and proportionate and effective.

Chapter 4: A human rights-based approach

Key points

- The introduction of age assurance measures and other technologies to prevent and mitigate harm to children associated with online pornography has the potential to impact a range of human rights.
- eSafety has considered the rights, best interests, and evolving capacities of children based on the United Nations Convention on the Rights of the Child and the Committee on the Rights of the Child's general comment no. 25 on children's rights in relation to the digital environment.
- Consistent with stakeholder feedback, eSafety has also considered the rights of other affected individuals and groups, including parents and carers, adult users of the internet, and sex workers, including performers and producers of online pornography.
- A proportionate and balanced approach should be taken to restricting children's encounters with and access to online pornography, which considers their best interests while respecting the rights of adults to consume and produce pornography in a safe and lawful manner.
- Measures to restrict children's access to online pornography should be guided by the United Nations (UN) *Convention on the Rights of the Child, in particular general comment (no. 25)* on children's rights in relation to the digital environment.
- Measures should:
  - protect children from online harms by considering their evolving capacities.
  - not discriminate against online users and should not restrict digital participation due to lack of access to identity documentation, or in-built bias in technologies.
  - protect children by not introducing risks to personal data security, privacy or identity.
- Businesses have a responsibility, alongside government, to prevent and mitigate online harms to users, as well as protect their digital human rights.
- The proactive delivery of awareness raising measures and provision of educational content by industry and government is crucial to supporting children, parents and carers, and other adults. These resources and initiatives should increase knowledge and understanding of online pornography and healthy sexual relationships, user-controlled safety measures and age restriction policies and technologies.

Overview

As articulated in the report's guiding principles, making the online world a safer, more inclusive, and accessible space is ultimately about fulfilling the human rights of those who inhabit it.

Under the *Online Safety Act 2021* (Cth) ('the Act'), the eSafety Commissioner must have regard to the United Nations (UN) Convention on the Rights of the Child (CRC) in the performance of her functions.[42] Measures to restrict children's access to online pornography, including the use of age assurance and other online safety technologies, relate to many of the rights articulated in the CRC. The implementation of such measures should also be guided by the CRC. The child rights experts who took part in our consultations also raised the importance of drawing upon the Committee on the Rights of the Child (CRC)'s general comment (no. 25) on children's rights in relation to the digital environment.[43]

eSafety has also drawn on UNICEF's discussion paper *'Digital Age Assurance Tools and Children's Rights across the Globe'* in considering the relevance and applicability of the CRC to the roadmap.[44] In addition, the Children's Rights and Business Principles report stresses the need for businesses to work with governments to take a human rights-based approach to focus on the impact of businesses on children and 'to both prevent harm and actively safeguard children's interests'.[45] The cross-jurisdictional and global reach of the digital environment means technology businesses have a greater role and responsibility in respecting and supporting children's rights.

Other stakeholders in our consultations – particularly privacy and broader digital rights advocate and those representing the rights of sex workers – emphasised that measures that restrict children's access to online pornography have human rights implications for adults as well as children. Consistent with their feedback, this chapter considers the rights of children, parents, carers and other adults regarding access to online pornography and the use of technological solutions to restrict children's access to harmful online content.

[42] Online Safety Act 2021 (Cth), s 24.
[43] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment.*
[44] UNICEF, *Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper*, 2021.
[45] United Nations, *Children's Rights and Business Principles,* 2012, https://www.unicef.org/documents/childrens-rights-and-business-principles

General principles on children's rights in relation to the digital environment (General comment no. 25)[46]

Participation and respect for views

Children

The digital environment is a critical platform that can provide children, in all their diversity, including those with disability and those of diverse genders, race, or socio-economic background, with an opportunity to be heard and amplify their views.

Article 12 of the CRC requires that governments and business seek out the views of children to understand children's experiences online and how they use technology to inform the design of systems. UNICEF has stressed that 'children should be consulted on their views about which platforms are appropriate for them to access, and should have their views taken into account before being denied access to online spaces or content on the basis of their age'.[47] As set out in chapter 3, this report draws on eSafety's quantitative and qualitative research with 16-18 year-olds, as well as discussions with members of the Youth Council, aged 13-24.

Parents and carers

The views and experiences of parents and carers of children should also be considered in the design, functionality and implementation of age assurance and other measures. These views should be used to create resources that empower parents to make informed decisions and have constructive conversations with their children, as discussed in chapter 13.

Other adults

All stakeholders should be meaningfully consulted on the risks, benefits and potential unintended consequences of online safety measures. As set out in chapter 3, this report was informed by consultation with a diverse array of stakeholders from multiple sectors, including digital platforms, the adult industry, digital rights and child rights advocates.

[46] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment.*
[47] UNICEF, *Digital Age Assurance Tools and Children's Rights Online across the Globe.*

Best interests of the child and most severe harms principles

Children

‘Best interests of the child’ is a dynamic concept generally assessed on a case-by-case basis.[48] All other rights listed under the CRC require that the ‘best interests of the child’ is the primary consideration.

The concept covers all aspects of children’s access to and participation in the digital environment – including the right to seek, receive and impart information safely, while being protected from harm, and it extends to the design and governance of the online environments they inhabit.[49] Children’s own views on their ‘best interests’ should be considered alongside parents and carers and other national bodies that oversee the fulfilment of children’s rights.[50]

Parents and carers

Parents and carers have primary responsibility for the upbringing and development of the child. Article 18 of the CRC requires that parents and carers be provided with appropriate assistance in their child-rearing responsibilities to support the best interests of the child, including when using digital technologies. Advice, support and tools should be offered by government and the technology industry to enhance understanding of the risks and opportunities for children in digital environments. This is further explored in chapters 12 and 13.

Other adults

A proportionate and balanced approach should be taken to restricting children’s encounters with and access to online pornography, which supports children’s best interests while respecting the rights of adults to consume and produce pornography in a safe and lawful manner.

Alongside the best interests of the child, the principle of addressing the most severe harm also guides digital technology companies in designing age assurance mechanisms. The *UN Guiding Principles for Business and Human Rights* advise that ‘business enterprises should first seek to prevent and mitigate those [infringements on human rights] that are most severe or where delayed response would make them irremediable.’[51]

[48] United Nations, *General comment No. 25 (2021) on children’s rights in relation to the digital environment*, paragraph 12.
[49] United Nations, *Convention on the Rights of the Child*, Article 3.
[50] United Nations, *General comment No. 25 (2021) on children’s rights in relation to the digital environment,* paragraph 13.
[51] United Nations, *Guiding Principles on Business and Human Rights,* p26.

Parental guidance and a child's evolving capacities

Children

As children get older the way they use technology changes, meaning the risks, harms and opportunities encountered in digital environments also change.[52] Systems or processes used to safeguard children from harmful content and conduct should respond to evolving capacities and establish age-appropriate measures for different age groups.

Age-appropriate measures for restricting access to online pornography and managing risks should be 'informed by the best and most up-to-date research available (from a range of disciplines'[53]) and consider the views of children. Chapter 5 includes discussion on children's views about the appropriate age of access, and chapter 13 discusses how educational resources should be tailored for children of different ages and stages.

Parents and carers

Online safety measures should engage parents and carers, supporting them to guide their child in accordance with their evolving capacities. Awareness-raising initiatives are necessary for expanding public knowledge of children's evolving autonomy and capacities and balancing this with protection from material harmful to their development. The educational needs of parents and carers, and tensions between parental guidance and a child's growing autonomy, are discussed in chapter 13.

Education

Children

According to the Committee on the Rights of the Child:

> 'it is of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance'.[54]

Children have the right to learn about the digital environment (including how to stay safe) and the right to harness the digital environment to access education (including on sexual health and respectful relationships). This is discussed further in chapter 13.

[52] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 12.

[53] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 12.

[54] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 105.

Parents and carers

As explored in chapter 13, parents and carers should be offered digital literacy education and training so they can support their child to engage with, and navigate, digital technologies safely.

Other adults

Adults should be able to access educational content about sex, sexuality or pornography. Measures to restrict children's access should not unduly restrict an adult's ability to engage in educational activities or resources.

Adults should have access to plain language information on why age assurance systems or other mechanisms may be necessary to view or post sexual content online, as well as information on the importance of minimising the risks of harm to children.

Resources should be culturally safe and incorporate an intersectional lens. Educators should also be upskilled to provide the right kind of guidance to children around age assurance processes and engage with these mechanisms themselves where necessary, as highlighted in chapter 13.

Right to non-discrimination

Children

Article 2 of the CRC requires that 'all children have equal and effective access to the digital environment in ways that are meaningful for them'.[55] This includes safe and free access to overcome digital exclusion. Mandatory measures to prevent children's access to online pornography must be designed to accurately assess the age of all children regardless of their ethnicity, colour, nationality, sex, language, disability or social status.

The use of biometric data or capacity testing to estimate age can result in varying levels of assurance, as explored in chapter 8. In some cases, the technology may fail to recognise characteristics of very light or dark skin and may not accurately assess the age for children who are close to 18 years of age. In addition, measures may not be accurate or appropriate for those with a disability, developmental delay, or low literacy.

Further, some age verification measures rely on the provision of identity documents. However, not all children have access to official documents or a fixed address. Other measures which require parent or carer input or consent risk excluding children without parents or carers who can engage with these processes.

[55] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 9.

This points to the need for multiple options for age assurance to be available to account for different circumstances. It also emphasises the importance of accuracy testing and the availability of review mechanisms where results are inaccurate or there are barriers to access. These factors are discussed in chapter 8.

Parents and carers

Online safety information and tools, including parental controls, should be affordable, accessible, and available to all, regardless of socioeconomic status, English language ability and digital literacy. Appropriately tailored resources, education and support should be provided to parents and carers to build their digital literacy and enhance children's safe and effective access to the digital environment.

Other adults

Measures should be designed to consider and remediate any unintended consequences for under-represented or marginalised groups. Age assurance measures should not inadvertently impact adults from culturally or linguistically diverse communities, those with disability, or those who lack access to government-issued identity documents from legally consuming or producing adult online content. Legally compliant sex workers, adult performers and producers of pornography operating should not be discriminated against due to their occupation.

As part of our consultations, eSafety spoke with sex workers and representative organisations to make sure the roadmap was informed by their expertise and perspectives.[56] Domestic adult industry stakeholders highlighted that local producers are often women, members of the LGBTIQ+ community and operating independently as sole traders or micro-businesses. Stakeholders requested these factors be considered to make sure measures that restrict children's access to online pornography are not designed solely with reference to larger, international 'tube' sites[57] and companies. This is discussed further in chapter 6.

Right to life, survival and development

Children

Digital technology has become an essential tool in children's development. The Committee on the Rights of the Child has stated that the digital environment 'may be vital for children's life and survival, especially in situations of crisis.'[58]

[56] See Appendix 5.

[57] A 'tube' site refers to a site which is free to view and relies on user-uploaded content, rather than the operator uploading content.

[58] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 14.

Digital technology is used for educational purposes and to provide critical information and services (including health and medical information, social services and news). It is also increasingly being used to provide social and familial connections and to develop interpersonal relationships which are critical to a child's development.

Preventing children (particularly younger children) from encountering online pornography protects and promotes their healthy development. The UN Children's Rights and Business Principles require that businesses take steps to make sure 'products and services are safe and seek to support children's rights'.[59] This includes proactively restricting access to online products and services that are harmful to, or otherwise not suitable for, children.[60]

Parents and carers

Parents and carers should be provided with training and advice on the appropriate use of digital technologies, parental controls, filters and age assurance tools to make sure they understand how their use may affect children's development, especially during early childhood and adolescence.[61] Training and advice for parents (and others, including educators) is discussed in chapter 13.

Other adults

Sex workers have the right to work and to do so within a safe environment. Digital technologies can provide a safe platform for sex workers to interact and engage with adult consumers. They can also provide a mechanism for adult consumers to explore their sexuality in the privacy and safety of their homes. It is important to make sure the design and application of age assurance or other measures does not place unreasonable burdens on sex workers from being able to engage and earn a living from their work and support themselves, such as by making it overly burdensome for consumers to access their websites.

In eSafety's consultations, we heard that measures to address adult content online often come at the expense of sex workers' ability to work lawfully and safely. While the local adult industry works within the Australian legal framework, the policies of large social media and other online services are often based on legal settings in other jurisdictions which may prohibit sex work.

In circumstances where sex work is not prohibited, sex workers shared they may still be de-platformed or censored on social media due to 'over-compliance' by online services. That is, where services will err on the side of removing permitted content rather than implementing more targeted measures to protect children. Stakeholders flagged they had few avenues to

[59] UNICEF, *Children's Rights and Business Principles*, 2012 p.24. https://www.unicef.org/documents/childrens-rights-and-business-principles
[60] UNICEF, *Children's Rights and Business Principles*.
[61] UNICEF, *Children's Rights and Business Principles*, p.26.

challenge these decisions or feed into relevant policies, pointing to the need for consultation and review mechanisms.

Stakeholders also emphasised that care should be taken to make sure measures for protecting children do not introduce risks for personal data security, privacy or protection of identity.

Protection and preservation of identity

Children, parents and carers and other adults

All stakeholders have an interest in ensuring that any requirement to provide identity data does not result in excessive data collection or monitoring, or any violation of privacy, freedom of thought or expression.

Since age assurance mechanisms often require some form of personal data to be given to online services or third-party age assurance providers, the retention and use of this data must be effectively regulated and protected. Special care and consideration must be taken to make sure the data collected as part of any age assurance process is protected from misuse and unauthorised disclosure and any collection of children's data must not be used to profile or target a child of any age for commercial purposes.

There is also an emerging right for individuals to an accurate, functional and unique digital identity which should also be considered (discussed further in chapter 9).[62]

Privacy

Children

Privacy is vital to children's agency, dignity and safety. Age assurance and parental control tools must proactively address the privacy concerns for children's data, including information on identities, activities, location, communication, emotions, health and relationships. Technological measures and associated processes must be secure and adhere to the principle of data minimisation. To make sure children can freely and safely benefit from the online environment, children should only be identified where it is necessary to prevent serious harm and where they (or their parents or carers) have consented to identification.[63]

[62] C Sullivan, '*Digital citizenship and the right to digital identity under international law*', Computer Law & Security Review, 32:474-481.

[63] UNICEF, *Digital Age Assurance Tools and Children's Rights Online across the Globe*, p.11.

Parents and carers

Parents and carers also have the right to privacy. Any use of their data to verify their child's age must be securely processed and protected from misuse or unauthorised disclosure. The data should only be used for the intended purpose it was provided.

Parents and carers should be given information on how their data may be used, stored and collected as well as information on how to protect their privacy and the privacy of their child.

Other adults

The International Covenant on Civil and Political Rights enshrines the right to protection against arbitrary and unlawful interference with privacy, correspondence and reputation, and to freedom of expression.[64] Age assurance systems should adhere to the principle of data minimisation to mitigate the risks associated with data collection. The data should only be used for the intended purpose for which it was provided. Adults should be given information on how their data may be used, stored or collected as well as information on how to protect their privacy. There should be adequate oversight of systems to ensure trustworthiness and to redress mechanisms for data or privacy breaches. The privacy reforms currently underway in Australia are discussed in chapter 9.

Freedom of expression, thought, association and access to information

Children

The CRC notes that 'content moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably rights to freedom of expression and privacy'.[65]

Measures established to protect children from accessing pornography must be lawful, necessary and proportionate to make sure they do not prevent children from enjoying the many and diverse benefits and opportunities the online environment provides for connecting with others, sharing ideas and expressing opinions. Protecting children's access to age-appropriate inclusive, accurate and relevant sexuality and health information is discussed in chapters 5 and 13.

[64] United Nations, *International Covenant on Civil and Political Rights,* 1966, Article 17. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[65] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, paragraph 56.

Parents and carers

Measures set up to prevent children from accessing online pornography should not interfere with a parent's or carer's ability to provide guidance and direction to their child in line with their evolving capacities.

Other adults

Measures should not prevent adults from legally consuming or creating pornographic content.

Protection from violence, abuse, neglect and exploitation

Children

As discussed in chapter 5, mainstream pornography often includes themes of violence, abuse and exploitation, and children's access to this content can be associated with harmful attitudes and behaviours. Pornography can also be used as a tool in the sexual grooming and exploitation of children.[66] Ensuring a child's right to be protected from sexual violence, abuse and exploitation must be considered alongside protecting and upholding their rights to freedom of expression, participation, education and access to information.

Parents and carers

Parents should be given advice and support to equip them with knowledge and skills that protect their child from being harmed by violent sexual content or exploitation online.

Other adults

The digital environment can provide a safe and private medium for adults to explore their sexuality as consensual consumers of online pornography. However, mainstream pornography can reflect and normalise sexual violence and abuse, particularly of women.[67] Everyone has the right to be protected from violence, abuse, neglect and exploitation.

Conclusion

eSafety has taken a human rights-based approach to developing the roadmap. The rights and needs of children, parents, carers and other adults are considered throughout this report. The report's evidence base, assessment of technical and non-technical solutions, and

[66] T Krone. *Child exploitation.* High tech crime brief no. 2. 2005. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/htcb/htcb2; Anti-Slavery Australia, *Behind the Screen: Online Child Exploitation in Australia*, 2017, https://antislavery.org.au/behind-the-screen-online-child-exploitation-in-australia/

[67] D Woodlock et al., *Second National Survey of Technology Abuse and Domestic Violence in Australia*, Curtain University WESNET, 2020. https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

recommendations reflect the broad range of rights enshrined in the UN Convention on the Rights of the Child and other international human rights instruments to which Australia is a signatory.

This chapter demonstrates the intersections between Australia's international human rights responsibilities and the roadmap's objective to establish measures which prevent children's access to online pornography and mitigate associated harms. Forthcoming chapters have been drafted with consideration of the roadmap's guiding principles and *UN Convention on the Rights of the Child (General Comment 25)*. eSafety has attempted to reflect these principles in its analysis and recommendations on:

- user choice and review mechanisms, technology accuracy standards and data protection and minimisation measures.
- consultation for developing educational resources, awareness raising and public information campaigns on technological solutions.
- protecting digital participation, addressing technological bias and the need for inclusive practice in designing technological solutions.

Part II – Understanding the issue

This volume of the report outlines the evidence provided to eSafety about children's access to online pornography – when and how they access it and the potential impacts associated with access. It also explores the relevant access points to online pornography within the digital ecosystem and how future technology trends may impact access and experiences.

Table of contents

Chapter 5: Evidence of harm and impacts of online pornography on children

Key points

- It is common for children to see online pornography. There is variation in when, where and how children see online pornography, as well as in the type and form of content they find. Their experiences with it, and feelings about it, also vary.
- When adolescent children intentionally seek out online pornography, doing so can be part of healthy sexual development and exploration. However, the content they encounter may not convey healthy messages. In addition, many children (including older teens) have seen online pornography unintentionally and have negative feelings about this.
- Online pornography is not homogeneous. However, studies point to a common, 'mainstream' form of pornography consisting of video content that targets a male heterosexual audience and forms a significant proportion of the global online pornography market. This content is readily accessible on major pornography 'tube' websites, which are some of the most accessed websites in Australia.
- Some studies have characterised the nature of mainstream pornography as containing, and normalising, depictions of sexual violence and derogatory, degrading sexual scripts about women. There is research which points to an association between pornography and harmful sexual attitudes and behaviours.
- It can be difficult to disentangle the potential impacts of online pornography from the broader context in which it is situated, as gender inequality, sexism and violence permeate all parts of our society.
- The research is complex and conflicting, and there are substantial gaps in the evidence base, particularly about the experiences of younger children, First Nations children, and those who are culturally and linguistically diverse. While further research is needed, the available evidence provides sufficient direction for initial action.
- Many factors can impact the potential for online pornography to harm children. There was greater agreement among the stakeholders we consulted about the potential for harm to younger children – as opposed to older teens – as they are more likely to lack the capacity, context and support to be able to critically analyse what they are seeing and temper its influence. This points to the need for an

approach which reflects the evolving capacities, needs, rights and best interests of children across different ages and stages, rather than a static approach for all children until they reach age 18.

Overview

Content warning

The following chapter contains descriptions of sexually explicit material, including the titles of online pornography videos and descriptions of the acts portrayed. It also contains discussions of gender-based violence and sexual aggression.

The Inquiry received many submissions expressing concern about the possible consequences associated with children and young people increasingly encountering online pornography. These submissions, and the Committee's findings, were also informed by a previous Inquiry conducted by the Senate Environment and Communications References Committee in 2016 on *Harm being done to Australian children through access to pornography on the Internet*.[68]

In response to eSafety's call for evidence and in subsequent consultations, some stakeholders raised questions about this evidence base. This included highlighting inconsistent, and potentially biased, definitions of harm; suggesting that a more multi-disciplinary range of resources should be considered; and calling out gaps in research about the diverse lived experiences of children and young people.

Accordingly, eSafety sought to establish an evidence base for this report which explores:

- The nature of online pornography
- Where, why, when and how children are viewing online pornography
- The evidence surrounding children's experiences with online pornography, including the associated harms and how children view their own experiences with online pornography and potential impacts
- The gaps in existing literature and outstanding questions.

This chapter draws on research submitted to eSafety through a call for evidence, stakeholder consultations, eSafety's own primary research with 16–18-year-olds, and supplemental desktop research.

[68] Senate Environment and Communications References Committee, *Harm being done to Australian children through access to pornography on the internet,* Parliament of Australia, 2016. https://www.aph.gov.au/parliamentary_business/committees/senate/environment_and_communications/online_access_to_porn.

While many genres and forms of pornography are available online, the focus of this chapter is on mainstream pornography – freely available on popular pornography tube sites and accessed by millions of Australian internet users. The broader evidence made available to eSafety shows it is common for children to have viewed online pornography, both intentionally and unintentionally. While participants in our research (16-18-year-olds) emphasised the importance of young people having agency over their own sexuality, they also highlighted that unexpected and unwanted encounters with online pornography are common for children and young people. This chapter explores a range of potential risks and impacts associated with children viewing online pornography, including its relationship with gender-based violence, children forming harmful views about sex and gender, and the general distress and discomfort created by unintentional encounters.

Consistent with the guiding principles informing this report, this chapter considers an interdisciplinary evidence base to understand the nature of the potential risks and harms to children, and the areas where there is greater or lesser evidence and agreement. This process revealed substantial diversity and complexity both in the nature of online pornography and in children's experiences with it. This complexity raises challenges in designing an approach to address the potential harms to children and reinforces the need for a multifaceted policy and regulatory response.

As noted in chapter 2, the scope of this report is limited to harms to children. However, some risks associated with online pornography identified in the literature (including the association with harmful views about women) also apply to adults. Additionally, many studies look at both children and young adults. For example, in one study, participants' ages ranged from 15 to 29).[69]

To the extent that age assurance, parental controls 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 overall, due to the increased likelihood of having received respectful relationships education prior to viewing such content.

However, technical solutions on their own will not address this issue. Starting online safety and respectful relationships education early and continuous reinforcement will support critical thinking skills and provide counter-narratives to harmful scripts in mainstream pornography, as discussed in chapter 13.

[69] M Lim, P Agius, E Carrotte, A Vella and 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.

What is online pornography?

To have an evidence-based discussion about online pornography, its impacts on children and effective mitigations for impacts, it is important to understand the nature and content of online pornography that children are likely to encounter.

As noted in chapter 2, for the purposes of this report:

Online pornography is online material that contains sexually explicit descriptions or displays that are intended to create sexual excitement, including sexual intercourse or other sexual activity.

This definition encompasses textual, visual and audio-visual material. It also encompasses material produced by both professional and amateurs, in both commercial and non-commercial contexts.

As noted in chapter 2, eSafety has opted for a broad definition of online pornography to enable this report to consider children's access to sexually explicit content in a range of contexts.

In a review of the last 50 years of academic research on the effects of pornography, it emerged there is not an agreed definition for pornography across the literature.[70] This should be kept in mind when considering the research presented throughout this chapter. A 2017 Australian Institute of Family Studies (AIFS) report also notes there is no singular type of pornography and there is substantial diversity in the forms that pornography can take (text, images, video and audio) as well as the content and production context.[71] This point was also raised throughout our consultations.

Mainstream pornography

The AIFS report concluded that there is a dominant form of pornography that is easily accessible online. This is predominantly video content which targets a male heterosexual audience and forms a significant proportion of the global pornography market. This content is often found on the home pages of the major free pornography tube sites – that is, sites which host large amounts of videos and allow user uploads (a model similar to YouTube).[72] Some studies have characterised the nature of mainstream pornography as containing, and

[70] A McKee, K Litsou, P Byron and R Ingham, *What do we know about the effects of pornography after fifty years of academic research?*, Routledge, 2022.

[71] A Quadara and A El-Murr, *The effects of pornography on children and young people*, Australian Institute of Family Studies, 2017. Available at https://aifs.gov.au/research/research-snapshots/effects-pornography-children-and-young-people.

[72] A Quadara and A El-Murr, *The effects of pornography on children and young people*.

normalising, depictions of sexual violence and degrading sexual scripts about women. eSafety acknowledges the wider discussions taking place on the extent to which mainstream pornography is reflective of broader societal inequality, sexism and gendered violence, rather than a contribution to it. The important work taking place through the *National Plan to End Violence against Women and Children 2022-2032* is discussed later in this chapter and elsewhere in this report.

Under the current classification regime, depictions of sexual or sexualised violence, sexually assaultive language and depictions which purposefully demean anyone involved in the activity for the enjoyment of viewers are 'Refused Classification'.[73] Based on research findings on the nature of 'mainstream pornography', there is substantial overlap with content currently deemed impermissible in Australia. More information about the legal framework applying to online pornography can be found in chapter 14.

Other pornographies

Beyond 'mainstream pornography', there are many other forms and genres of pornography raised during consultation:

- *Different mediums* – some participants in our consultation focus groups talked about written erotica (in particular, content hosted on fanfiction site Archive of Our Own or AO3)[74] as a form of online pornography they were familiar with. Other forms of online pornography include illustrated/cartoon content, such as manga. eSafety has previously received complaints about both fan fiction and manga from members of the public reporting sexually explicit material.
- *Amateur versus professional* – online pornography can be produced by individuals or by production houses. Amateur content may be for financial purposes or it may be created for other reasons, including artistic expression.
- *Ethical* – some stakeholders raised examples of commercially produced pornography that seeks to avoid the issues identified in 'mainstream pornography'. Content of this genre may depict a variety of body types, genders and races and show negotiations of consent and safer sexual practices.[75] The production context and treatment of performers is also a factor.

[73] *Guidelines for the Classification of Films 2021.*

[74] AO3 is a non-profit open-source website hosting fanfiction and other works including audio stories and art, operated by the Organization for Transformative Works. Fanfiction is fictional writing by fans based on an existing work of fiction. Written erotica content not produced for commercial purposes is likely to have a significantly different risk profile compared to mainstream video content.

[75] A McKee, A Dawson and M Kang, 'The criteria to identify pornography that can support healthy sexual development for young adults: Results of an international Delphi Panel', *International Journal of Sexual Health*, 2023, 35(1):1-12, DOI: 10.1080/19317611.2022.2161030

- *Queer* – many stakeholders talked about online pornography made by and for the LGBTIQ+ community, and the value it can provide in terms of expression, education and self-realisation.
- *Feminist* – some stakeholders raised feminist pornography – which centres female perspectives, desires, pleasure and consent – as a counterbalance to mainstream pornography.

This is not meant to represent an exhaustive list of online pornographies, but rather to illustrate that there is range of content, genres and forms of online pornography children may encounter online.

Content analysis

Analysis of the content of online pornography is limited due to several factors, including the volume and diversity of content available and the speed at which new content is produced. Definitional differences, sampling approaches, and a lack of standardisation may explain variations in studies which examine violence and aggression in mainstream pornography.

A 2021 UK study analysed the titles of more than 130,000 videos from XHamster, XVideos and Pornhub. It found 12% of videos shown to first-time users on a homepage described sexual activity that constitutes sexual violence.[76] The study prioritised the analysis of the entire sample of content, rather than conducting a content analysis of the images, which would not have been possible given the sample size.

In 2019, the New Zealand Classification office conducted a content analysis of the 200 most popular videos on Pornhub for New Zealand viewers. This study found 10% of videos contained aggression. In contrast, another study cited by the Classification Office found 36.8% of a random sample of videos were coded for physical aggression. The New Zealand study suggested that differences in coding for aggression and different approaches to sampling the content were likely to explain the disparate findings. This demonstrates the challenges facing researchers in conducting content analysis of mainstream pornography at scale.

eSafety supports suggestions across the literature that more research is needed to understand the modern online pornography landscape and to address the significant lack of evidence about children’s actual engagement with online pornography.

eSafety has reviewed the content that is accessible on the home pages of the most-accessed pornography sites from Australia. We suggest this could be illustrative of the content children

[76] F Vera-Gray, C McGlynn, I Kureshi and K Butterby, *‘Sexual violence as a sexual script in mainstream online pornography’,* British Journal of Criminology, 2021, 61(5):1243-1260.

are most likely to encounter, including sexual violence, harmful gender stereotypes and illegal behaviour. However, we acknowledge this will not be reflective of all children's experiences.[77]

These are video titles on the homepages of the five most accessed pornography sites in Australia as at February 2023

- 'Step mom teaches step daughter and step son how to fuck'
- 'Young slave get punishes [sic] with baseball bat'
- 'Stepdad and stepdaughter. Risky cum in her mouth.'
- 'I like to sit on my stepson's legs to feel his dick while we play video games'
- 'Sweet brunette teen vacation sex – perfect girlfriend'
- 'Pervy step parents watch bro cum inside his stepsis'
- 'It feels so right to fuck my step sisters tight pussy'
- 'Teaching my stepdaughter please a man'
- 'Public anal creampie'

[77] Similarweb, *Top websites ranking: Most visited websites in Australia*, accessed February 2023. https://www.similarweb.com/top-websites/australia.

When, where and why are children encountering pornography?

The activities children engage in online, the risks and harms they face, and their capacity to deal with these risks and harms evolve over time.

eSafety conducted quantitative and qualitative research in 2022 with over one thousand 16-18-year-olds about their views on, and experiences of, online pornography and age verification. Our survey found that most participants had encountered online pornography (75%) and those encounters had started well before 18.[78]

It is important to acknowledge that children's unique experiences may be informed and influenced by a wide range of personal and societal factors. It would be inaccurate to characterise the impact of online pornography on children as if on a homogenous group.

As noted below, children's experiences with online pornography are likely to change as they grow older and mature. In line with the stakeholders we consulted, it is eSafety's view that measures to protect children should reflect children's evolving capacities.

Limitations of available literature

- Many studies into the prevalence of accessing online pornography are based on 'non-probability convenience samples'. A non-probability-based sample means not everyone has an equal chance of being selected to participate in the research, and therefore they are not representative of the general/target population. That is, the extent to which a sample mirrors a target population and reflects characteristics of age, gender, ethnicity and socioeconomic status. This makes it difficult to generalise the findings from these studies to broader populations.
- A representative sample can be difficult to achieve with current participant recruitment techniques, especially for children and young people who cannot be accessed directly through, for instance, a randomised phone number generator.
- Achieving a representative sample of children and young people is also challenging due to the necessarily strict ethics standards. Parental consent is required for those who cannot consent as 'mature minors' (usually under 16). This can limit

[78] While the survey was conducted Australia-wide and the sample included young people with disability, those who speak a language other than English at home, LGB+ young people, trans and gender diverse young people, and Aboriginal and Torres Strait Islander young people – the number of Aboriginal and Torres Strait Islander and trans and gender diverse participants was too small to provide for separate analysis in this chapter.

potential participants to those whose parents are comfortable discussing issues like pornography with their children.

- Moreover, capturing the perspectives of Aboriginal and Torres Strait Islander children and young people, or children and young people from culturally diverse communities, requires researchers from that community to lead or shape the study to ensure it is culturally safe.
- Research into the prevalence of children and young people seeing online pornography is often inconsistent in defining what is being measured. For example, while some studies differentiate between intentional viewing and accidental or unintentional viewing, some do not. The duration of viewing is also inconsistently measured and included in research. Definitions of what is meant by 'pornography' are also inconsistently provided, and when they are, definitions and age ranges often vary, making comparisons between studies can be difficult.
- This means conclusions should consider the limitations of the literature and studies should be compared with care.

When do children first encounter online pornography?

Most participants in our survey first encountered online pornography well before the age of 18.[79]

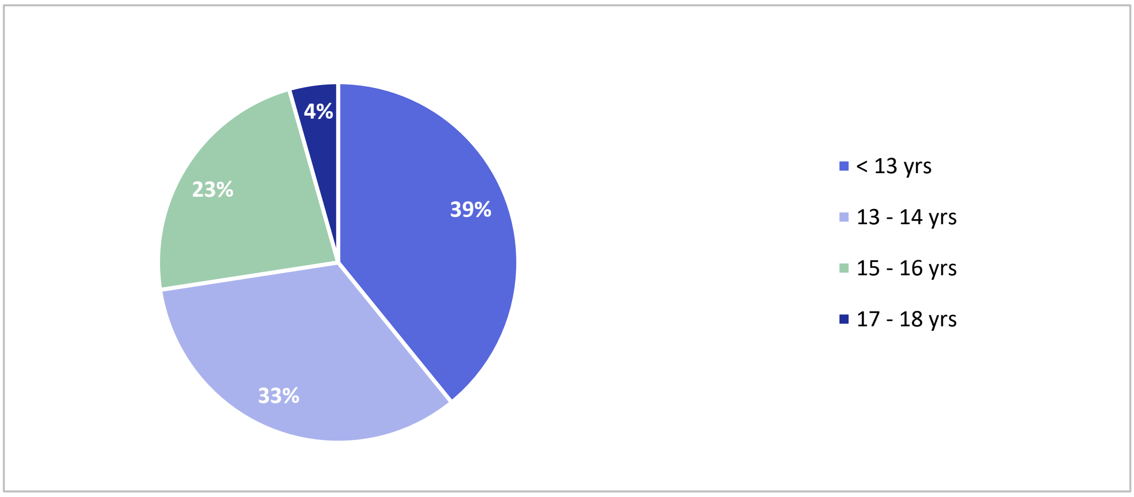


Figure 1 - eSafety research: Thinking about the first time you saw online pornography, how old were you at the time? (survey sample, unweighted, young people who have seen online pornography n=751)

[79] Online pornography was defined for survey participants as: textual, visual and audio-visual sexually explicit material that is primarily intended to sexually arouse the audience. This can include representations of images of nudity or semi-nudity, implied sexual activity and actual sexual activity that is uploaded, accessed and shared via online platforms. This does not include the sending or receiving of nudes or nude selfies, also known as ‘sexting’.

Summary of experiences by age group

Children under 10

Our survey found 8% of participants who had seen online pornography first did so when they were under 10 years old.[80]

If our survey results were a class of 20 children under 10, at least one child would likely have already encountered online pornography.

Across the literature, it is relatively uncommon for children to encounter pornography before the age of 10.

However, consultation participants, including education departments and third-party education providers, reported anecdotal experiences of children viewing or sharing pornography as young as 6 or 7 in a school setting, and there is a perception that the age of children encountering online pornography is getting younger.[81]

Research is very limited as to the nature of children's access to online pornography at this age and there is not a great deal of evidence about the specific impacts of viewing pornography for this group due to ethical and other limitations about conducting research with this age group.

Stakeholders suggested there is a particular risk of harm to this age group as they often have not received any relevant prior education about sex, respectful relationships and what to do if they see online pornography.

Most children at this age are using shared family devices. This may create opportunities for more robust safety settings and supervision. Children of this age generally cannot have their own accounts for many online services, including social media services (which can be a conduit for accessing online pornography). However, as discussed in chapter 8, enforcing relevant minimum ages requires services to employ effective age assurance measures.

[80] The sample size for young people who first saw online pornography before the age of 10 was very small in our survey (n=64). Findings are indicative only and must be interpreted with caution.

[81] These observations reflect the experience of education providers and education authorities. Of note – most research with young people about pornography includes participants that are 15+ and they are reflecting on their own experience from potentially 5 or more years ago. Technology, and in particular patterns of usage on the internet shift incredibly fast – and there is a risk that their experiences no longer reflect the experience of current children under 10. We have used the observations from consultation participants to consider the gap, however, we acknowledge the limitations of such evidence.

Where children can have accounts (for example, on Apple devices or Google accounts) these can be subject to parental controls limiting apps and web-browsing (see chapters 8, 11 and 12 for further discussion).

Ages 10-12

> Our survey found 9% of participants who had seen online pornography first did so when they were 10 years old, 7% were 11 years old and increasing to 15% at 12 years old.
>
> **If our survey results were a class of 20 children aged 10-12, at least 5 would have already encountered online pornography.**

Research about children's experiences with pornography at this age is also limited. According to Australia's National Research Organisation for Women's Safety (ANROWS), irregular viewing of pornography among children 10-13 and younger can be 'concerning sexual behaviour', and chronic pornographic interest can be 'very concerning sexual behaviour'.[82]

Our survey found that participants who reported encountering online pornography frequently, were more likely to have first encountered it at a younger age: 89% of young people who encountered online pornography several times per day, had first encountered it before 13 years of age.[83]

Research in the UK found that those who viewed online pornography at age 11 or younger were statistically significantly more likely to access pornography frequently.[84]

When reflecting on how they had encountered online pornography, our survey found that those who first encountered online pornography before 13 were also significantly more likely to say that they had subsequently intentionally accessed it (72% vs 61%).

Children in this age group may be more likely than younger children to have unsupervised access to devices. While many online services have minimum ages of 13+ to sign up for accounts, research has found that many children provide false ages. Research commissioned by Ofcom found 60% of children under the age of 13 who use social media accounts have their own profiles, despite not

[82] A Quadara, W O'Brien, O Ball, W Douglas and L Vu, *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours*, ANROWS, 2020. https://www.anrows.org.au/publication/good-practice-in-delivering-and-evaluating-interventions-for-young-people-with-harmful-sexual-behaviours/.

[83] eSafety, forthcoming.

[84] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023. https://www.childrenscommissioner.gov.uk/resource/a-lot-of-it-is-actually-just-abuse-young-people-and-pornography/.

	being old enough – and 39% of children aged 8-12 with a social media profile have a user age of 16+.[85] This means age-specific safety measures are not properly enabled.
Ages 13-15	Our survey found 47% of participants who had seen online pornography first encountered it when they were 13 - 15 years old. Most children in our survey encountered pornography for the first time in this age range. **If our survey results were a class of 20 children aged 13-15, at least 12 would have already encountered online pornography. 86% of the participants in our survey who had seen online pornography on at least one occasion first encountered it before the age of 16.** The average age of children encountering online pornography in our survey was 13.1 years.[86] Similarly, the 2021-22 Australian National Survey of Secondary Students and Sexual Health (SSASH) survey found that the average age for viewing pornography was 13.6 years old.[87] At 13, children can create their own social media accounts, according to the terms of service or community rules of most major services. At this age, more children are using their own devices, and doing so without supervision. As discussed in chapter 11, they can opt out of parental controls on Apple and Google devices. According to ANROWS, for children 14-18 the intentional viewing of pornography may be an age-appropriate sexual behaviour.[88] 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 material, and whether the material is age-appropriate for them to view.

[85] Ofcom, *Children's Online User Ages Quantitative Research Study*, 2022, [PDF 992.6 KB] https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart-pack.pdf.

[86] eSafety, forthcoming.

[87] J Power, S Kauer, C Fisher, R Bellamy and A Bourne, *7th National survey of Australian secondary students and sexual health 2022*, The Australian Research Centre in Sex, Health and Society, La Trobe University, 2022. https://www.latrobe.edu.au/arcshs/work/national-survey-of-secondary-students-and-sexual-health-2022.

[88] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours,* 2020.

Ages 16-18	Our survey found 10% of participants who had seen online pornography first encountered online pornography when they were 16 years old. **Only 4% were 17 or 18 when they first encountered online pornography**. **If our survey results were a class of 20 children aged 16+, at least 14 would have already encountered online pornography before the age of 18.** Across most states and territories in Australia, the age of consent for sex is 16.[89] One in two young people in our survey agreed this should be a relevant consideration in whether young people can access online pornography. While choosing to view sexually explicit content may be part of healthy sexual development – the content young people are viewing may not represent healthy behaviours and messages (e.g., content which depicts harmful narratives about gender).

Comparison with other studies – age of first access

A rapid review of evidence in international literature found that encountering or accessing online pornography increases with age. [90] However, there is inconsistent evidence regarding age of first encounter, with evidence this can range from 10 to 17 years. Other studies submitted to eSafety found similar age ranges.

- Qualitative research conducted in 2017 with men in the US aged 18-32 with non-exclusive sexual orientations[91] found that participants saw pornography from an early age, with the average age of first encounter being 14 years old and the youngest aged 8.[92]
- A nationally representative study with 14–17-year-olds in New Zealand in 2019 found that of those who had ever seen pornography (67%), the average age of first seeing pornography was just under 13 years, and the average and median age by which regular

[89] Australian Institute of Family Studies, *Age of consent laws in Australia*, 2021. https://aifs.gov.au/resources/resource-sheets/age-consent-laws-australia.

[90] M Horvath, L Alys, K Massey, A Pina, M Scally & J Adler, *'Basically ... Porn is everywhere': A rapid evidence assessment on the effects that access and exposure to pornography has on children and young people*, 2013. https://repository.canterbury.ac.uk/item/870qz/-basically-porn-is-everywhere-a-rapid-evidence-assessment-on-the-effects-that-access-and-exposure-to-pornography-has-on-children-and-young-people.

[91] In this study, this description refers to participants who don't identify exclusively with one label.

[92] M McCormack and L Wignall, *'Enjoyment, exploration and education: Understanding the consumption of pornography among young men with non-exclusive sexual orientations'*, *Sociology,* 2017, 51(5):975-991, DOI: 10.1177/0038038516629909.

(monthly, weekly, or daily) viewers started looking at porn this often was around 14 years.[93]

Our survey found that several demographic factors impacted the age young people 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 (47%) were significantly more likely to first encounter online pornography before the age of 13 compared to the overall sample (39%).[94]

Our research did not reveal significant differences between genders. However, research submitted to the call for evidence suggested that boys may access online pornography at a younger age, on average, than girls. Two of these studies, conducted in Australia in 2017 and 2020, found that the median age at first pornography viewing was 13 years for men and 16 years for women.[95]

Comparison with other studies – prevalence and frequency of access

> 'Kind of like there's no escaping it in a way like you're always surrounded by it' – eSafety focus group participant, 18.

In the *2022 Australian National Survey of Secondary Students and Sexual Health (SSASH) survey,* 85.7% of respondents (aged between 14-18) reported that they had viewed pornography.[96]

Our survey found no significant difference between the proportion of boys (79%) and girls (72%) who had encountered online pornography. For participants in our survey who had seen online pornography on at least one occasion, 86% first encountered it before the age of sixteen. However, other studies revealed significant gender differences: a nationally representative Australian study published in 2018 found that among 3,089 16–17-year-olds, 34% of girls and 73% of boys had ever seen pornography.[97]

While studies often reveal high proportions of children have seen online pornography at least once, there is more variation in the frequency of access. The SSASH survey found 14.7% of respondents viewed pornography monthly, 19.5% weekly and 14.1% daily or almost daily.[98]

[93] C Henry and H Talbot, *'The complexities of young New Zealanders' use and perceptions of pornography: A quantitative survey in context',* Porn Studies, 2019, 6(4):391-410, DOI: 10.1080/23268743.2019.1656544.

[94] eSafety, forthcoming.

[95] Non-representative sample of 15-29 year olds in Lim et al., *Young Australians' use of pornography and associations with sexual risk behaviours*. Non-representative sample of 15-20 year olds in OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020, available at: https://www.ourwatch.org.au/resource/pornography-young-people-and-preventing-violence-against-women-background-paper-2020/.

[96] Power et al, *National survey of Australian secondary students and sexual health.*

[97] Lim et al., *Young Australians' use of pornography and associations with sexual risk behaviours*.

[98] Power et al, *National survey of Australian secondary students and sexual health.*

Another quarter (25.1%) reported that they did not view pornography at all in the past year, and a similar proportion (26.6%) reported viewing pornography less than monthly in the past year. [99]

Another nationally representative study in Australia with 16–17-year-olds found one in four (24%) boys and one in twenty girls (4%) reported watching pornography weekly.[100] Research published by the England Children's Commissioner in 2023 found 21% of boys had intentionally viewed pornography at least every day in the two weeks prior to the survey, while 7% of girls had done so. Notably, the participants in this study ranged from 16-21, so much of this access would have been permissible under law.[101]

Where do children see online pornography?

Our survey found that pornography sites were the main place participants had seen online pornography – 70% of respondents who had seen pornography, had done so on such a site. This was more common for older participants aged 18 (77%) and 17 (71%) compared to 16-year-old participants (59%).

Other common places 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%).

Boys were significantly more likely to have seen content on a pornography site compared to girls (76% vs. 65%). Girls were significantly more likely compared to boys to have seen pornography via social media feed (39% vs. 27%), an ad on social media (31% vs. 20%), and social media direct message (27% vs. 15%).

[99] Power et al, *National survey of Australian secondary students and sexual health.*

[100] D Warren and N Swami, 'Chapter 5: Teenagers and sex', *The Longitudinal Study of Australian Children*, Australian Institute of Family Studies, 2018. https://aifs.gov.au/sites/default/files/publication-documents/lsac-asr-2018-chap5-teenagers-and-sex.pdf.

[101] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.

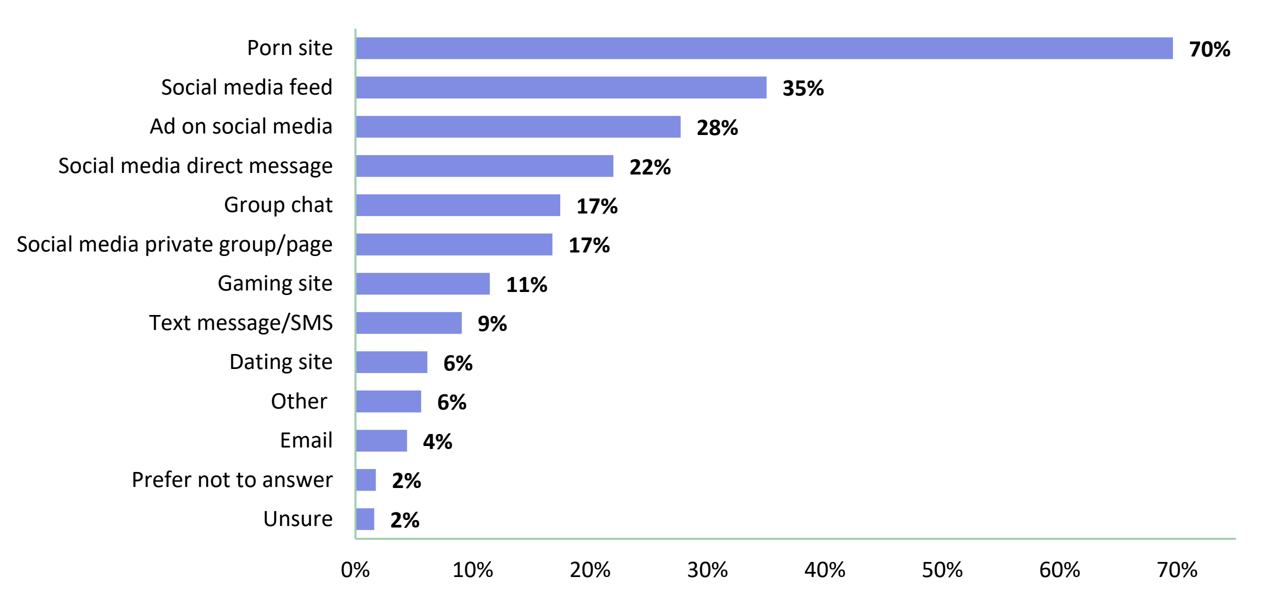


Figure 2 Where have you seen online pornography in general? (survey sample, unweighted, young people who have seen online pornography n=751).[102]

While pornography sites are the most common place where participants had seen online pornography, a significant number of participants had seen this content on social media sites (as posts, ads or in direct messages) or other services. This suggests it would be under-inclusive to only apply age assurance measures to pornography sites. Other complementary measures, including more robust content moderation on social media and parental controls on devices, could also address this access.

In a 2015 Australian qualitative study with 15–20-year-olds, participants described pop-ups and social media sites as common ways pornography is encountered and shared.[103] In our focus groups, participants told us they had seen pornography through anonymous text and video chat sites, pop-ups on torrenting sites, movie streaming/pirating sites and gaming sites. Pornography was also shown to them by peers.

> '…I think it's [pornography] pretty accessible across most platforms, including reddit Instagram etc.' – eSafety focus group participant, 17
>
> 'I've found too much of it on websites I would use in places like Twitter or Reddit. I have actually seen some slip through the cracks on TikTok, out of all places' – eSafety focus group participant, 18

[102] Of those that saw pornography on dating sites: 35% were 16yrs and 37% were 17 years old. Most dating sites have an age limit of 18+ to join the service.
[103] S Walker, M Temple-Smith, P Higgs and L Sanci, ''It's always just there in your face': young people's views on porn', *Sexual Health*, 2015, 12(3):200-206, DOI: 10.1071/SH14225

> ‘Yeah, snapchat is full of those sorts of things especially now with fake accounts being made for the purpose of trying to get teens to access porn which is sometimes paid content too’ – eSafety focus group participant, 16
>
> ‘Yes, often you will just be trying to do something on a different website like watch normal videos or find information and there will be a pop up of ‘hot milfs [mothers I'd like to f***} in your area’’ – eSafety focus group participant, 17
>
> ‘There are some sites where one minute you are looking at some nice art, and the next, its porn, which is really bad if you previously thought the place was somewhere a kid could go without having to worry about unexpected surprises’ – eSafety focus group participant, 18

A recent survey commissioned by the Children’s Commissioner in England found that 41% of participants (16-21) who had seen online pornography had viewed it on Twitter. This was more than dedicated pornography sites (37%) and other social media sites (Instagram 33%, TikTok 23%, Reddit 17%).[104]

Children sharing links to content in group chats or in social media messaging was also commonly raised among stakeholders in our consultations. Stakeholders who provide third-party educational presentations for schools believe there has been an increase in reports from teachers and students of peer-to-peer sharing of pornography in school and school-adjacent environments (such as on the school bus).

Our survey found one in three (34%) young people first encountered online pornography when it was shared with them via their peers and/or social networks (e.g., when someone sent it to them, showed them or it appeared in a group chat).[105]

Why are children accessing online pornography?

> ‘I think in an ideal world you would only encounter it by choice’ – eSafety focus group participant, 16

Children view online pornography both intentionally and unintentionally online and often feel differently about these experiences.

[104] UK Children’s Commissioner, *‘A lot of it is actually just abuse: Young people and pornography*, 2023.
[105] This may also include a proportion of young people who requested that their peers (or ‘someone’) show them or send them the content.

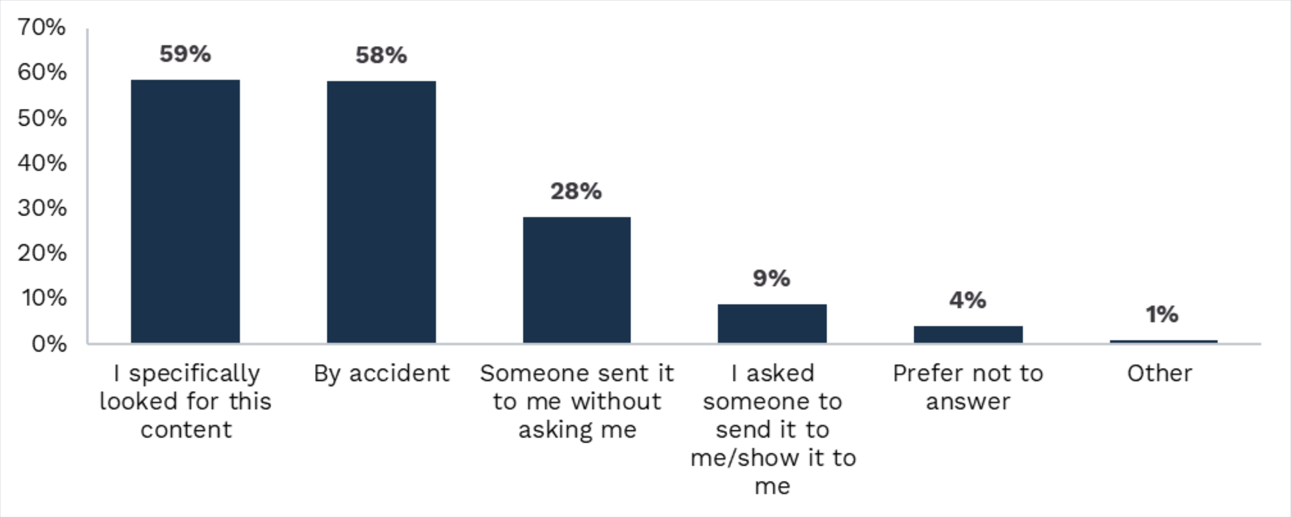


Figure 3 How have you seen online pornography in general? (selecting all that apply) (survey sample, unweighted, young people who have seen online pornography n=751)

Understanding intentional access

eSafety acknowledges the binary labels of ‘intentional’ or ‘unintentional’ may fail to capture the nuanced spectrum of interactions children have with online pornography, such as when children intentionally click on links out of curiosity without fully understanding what they are accessing. They may also be served content via a recommendation algorithm which suggests content based on the type of content they have previously engaged with. This can include circumstances where content that is intentionally accessed is immediately followed by content a person did not intend or expect to see (e.g., auto-play videos).

During our consultations, several stakeholders raised concerns about the language used to distinguish between intentional and unintentional (or accidental) access. Some were concerned that a focus on intentional engagement could be seen as stigmatising or placing blame on children who seek out content. Others were concerned that labelling engagement as ‘unintentional’ or ‘accidental’ does not reflect the experience of users and the responsibility of online services relating to targeted content.

However, most stakeholders expressed the view that understanding the context in which children encounter pornography is important for establishing potential risks, harms and proportionate and effective interventions. They highlighted that while age-based access restrictions may seek to address the issue from the supply-side, understanding the full range of motivations for children to engage with pornography can help us to address the issue from the demand-side as well. For example, we heard that children’s reliance on pornography to learn about sex can be reduced by making sure sexuality education is more accessible, inclusive and relevant.

In explaining children’s reasons for engaging with pornography, we are not endorsing its use for these purposes, but rather seeking to establish the evidence base to inform proportionate and effective responses. 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.

Our survey found most children encountered online pornography unintentionally the first time. The most common pathways for access:

- two in five (40%) children first encountered online pornography when it appeared online (e.g., ads on social media or a gaming site, or it popped up while searching for something else or in their social media feed)
- one in three (34%) children first encountered online pornography when it was shared with them via their peers and/or social networks (e.g., when someone sent it to them, showed them or it appeared in a group chat).[106]

Almost one in three (30%) participants in our survey first encountered online pornography unintentionally (when it appeared online or when it was shared with them) before they were 13.[107]

> 'I was pretty sheltered as a kid in terms of internet usage but still experienced pop-ups and whatnot' – eSafety focus group participant, 18

While many children see online pornography unintentionally the first time, unintentional access continues to feature in their experiences online as they progress through adolescence. Many focus group participants agreed that seeing pornography unintentionally was a common experience. This was also reflected in our survey findings.

Unintentional viewing

Inadvertent pathways to accessing online pornography can include searching for information, including sexual health or relationships education, pop-up ads or appearances in social media feeds. Children can also see pornography without actively searching for it by having someone share the content or links with them directly or in a group chat or be shown content on another person's device. While some studies consider being sent links as intentional access (given the requirement to choose to click on the link),[108] others may categorise this as unintentional access, as the child did not seek it out and may not have known what the link contained.

[106] This may also include a proportion of young people who requested that their peers (or 'someone') show them or send them the content.

[107] OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020.

[108] Quadara and El-Murr, *The effects of pornography on children and young people*, 2017.

Children and young people in particular face risks from recommender systems serving them content and accounts that may not be age appropriate. [109]

> 'A lot of social media platforms have terrible moderation, so this stuff can slip through the filters and get recommended to you' – eSafety focus group participant, 16

These systems can contribute to children unintentionally viewing online pornography.[110] For example, reports emerged in 2017 that young people were being drawn to YouTube videos depicting children's characters engaging in sexual and violent activity. This content was found to be embedded in popular children's channels and designed to be promoted to children.[111] New research indicates that children are being led to inappropriate content through free videos on apps like YouTube and TikTok. It interviewed parents who felt children required constant supervision due to the risk that YouTube's 'autoplay' feature would transition to inappropriate content.[112] Reports have also emerged of popular YouTube channels and videos being bombarded with comments encouraging users to visit pornography sites.[113]

Observations emerged from our focus groups describing almost an omnipresence of pornography in participant's online worlds. In particular, the prevalence of online pornography meant unintentional encounters were described as 'frequent' and 'unavoidable'. 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%).

> 'While there's no shame on those who are actively seeking out pornographic content for their own needs, I have had discussions with my friend group and none of us found porn for the first time on our own, we were all exposed to it one way or another' – eSafety focus group participant, 18

[109] Recommender systems, also known as content curation systems, are the systems that prioritise content or make personalised content suggestions to users of online services. A key component is the recommender algorithms, or computing instructions, that determine what a user will be served based on many factors. This is done by applying machine learning techniques to the data held by online services, to identify user attributes and patterns and make recommendations to achieve particular goals.

[110] V Jaynes and I Wick, *Risky by Design: Recommendation Systems*, 5Rights Foundation, 2022. https://www.riskyby.design/risks.

[111] R Brandom, *Inside Elsagate: the conspiracy-fueled war on creepy YouTube Kids videos*, The Verge, 2017. https://www.theverge.com/2017/12/8/16751206/elsagate-youtube-kids-creepy-conspiracy-theory.

[112] Department of Infrastructure, Transport, Regional Development, and Communications, *Report on classification usage and attitudes research*, 2022. https://www.classification.gov.au/about-us/research-and-publications/classification-usage-and-attitudes-2022.

[113] T Saunders, *YouTube comments bombarded with porn and scam links targeting channels with millions of young fans*, inews, 2022. https://inews.co.uk/news/technology/youtube-comments-spam-porn-scams-1571639.

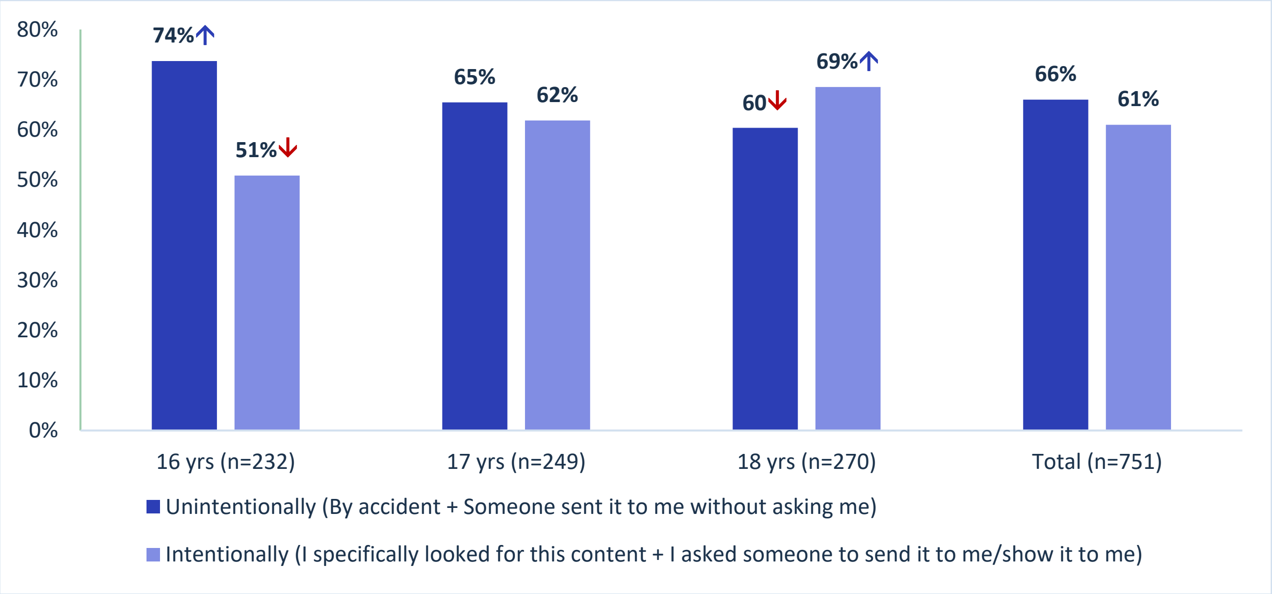


Figure 4 How have you seen online pornography, in general? By age today (survey sample, unweighted, young people who have seen online pornography n=751) Note: arrows denote results with a statistically significant difference.

Research published in 2023 by England's Children's Commissioner asked children 11-17 of all the pornography they had seen online, how much they had seen intentionally compared to seeing it by accident.[114] For younger children (aged 11-13), 62% felt they had seen more content unintentionally, while 18% felt they had seen more content intentionally, and 19% felt it was mixed. In comparison, 46% of 16-17-year-olds felt they had seen more content unintentionally, 29% felt they had seen more content intentionally, and 25% felt it was mixed.

[114] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.

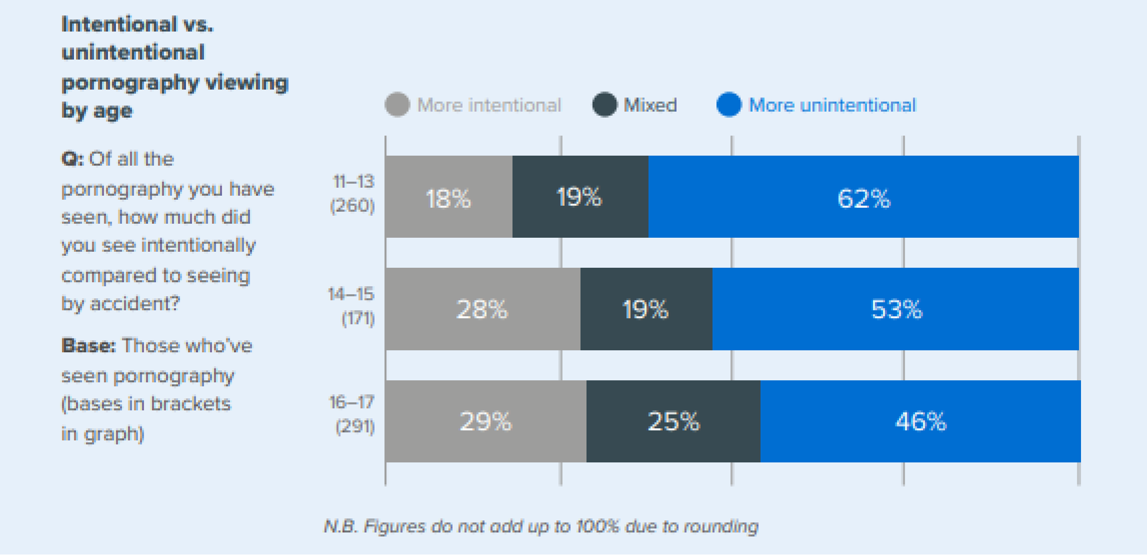


Figure 5 UK Children's Commissioner, 'A lot of it is actually just abuse' Young People and Pornography

These findings point to differing experiences children have online as they grow up and suggests more granular measures which reflect children's evolving capacities are required to promote children's rights and best interests across different ages and stages.

Research submitted to eSafety recognised sexual agency, or being in control of one's own sexuality, as an important domain of healthy sexual development for children and young people.[115] 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 on being able to choose when they intentionally view pornography and choosing when not to see pornography (e.g., content encountered unintentionally in online locations outside of pornography sites).

> 'I would like them [young people] to be able to feel good about it [seeing online pornography], because the only time they'd see it is if they WANTED to see it, and looked for it, rather than it being shoved into their faces by strangers' – eSafety focus group participant, 18
>
> 'As long as it is consensual then do what you want with your body' – eSafety focus group participant, 16

[115] A McKee, K Albury, M Dunne, S Grieshaber, J Hartley, C Lumby and B Mathews, *'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*, Leiden University Faculty of Law, 2019. https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-privaatrecht/jeugdrecht/xin-jiang---age-verification-porn-tube-sites-and-childrens-rights.pdf.

> 'Yeah, I think when it's on sites that people are specifically searching for it is nowhere near as dangerous as when it get sent out unconsensually (sic)' – eSafety focus group participant, 17

Without discounting the importance of agency, some research cautions that a focus on young people's autonomy and decision-making in discussions of pornography should not be at the expense of highlighting how pornography can shape social norms around gender and sexual violence – for children, young people and adults.[116] That is, children may choose to engage with pornography and find it a pleasurable experience without being conscious of how it may be influencing their preferences, attitudes and behaviours in a way that is ultimately harmful.

Intentional viewing: why do children seek out pornography

Research suggests that children choose to watch online pornography for several reasons. These can include curiosity, boredom, relaxation, education, as a joke and sexual arousal.[117] Our survey asked 16-18-year-old participants how they most recently encountered online pornography, and 52% of respondents had specifically looked for the content.

Out of curiosity and for sexual exploration or arousal

Academic stakeholders emphasised during the consultation process that it is common, and part of healthy sexual development, for children and young people to seek out sexual material post-puberty.

Our Watch's 2020 survey (15-20-year-olds) found that participants' primary motivation for first seeking out online pornography was curiosity (78%) while 26% reported sexual stimulation as their primary motivation.[118]

> 'Young people before exposure don't really search for it, but once introduced people are curious' – eSafety focus group participant, 16
>
> 'A lot of people show their friends this kind of stuff even if it's as a joke at first but quite often people get curious and start searching themselves' – eSafety focus group participant, 16

[116] M Coy and M Tyler, 'Pornography and sexual violence: Reflection on policy debates around age, gender, and harm', in M Horvath & J Brown (eds), *Rape: Challenging contemporary thinking – 10 years on* (2nd ed.), Routledge, 2022.

[117] F Attwood, C Smith and M Barker, *'I'm just curious and still exploring myself: Young people and pornography'*, New Media & Society, 2018, 20(10):3738–3759, DOI: 10.1177/1461444818759271; Henry and Talbot, 2019; S Healy-Cullen, J Taylor, K Ross, and T Morison, *'Youth encounters with internet pornography: A survey of youth, caregiver, and educator perspectives'*, Sexuality & Culture, 2022, *26*(2):491-513, DOI:10.1007/s12119-021-09904-y.

[118] OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020.

Participants in our focus groups said seeing online pornography intentionally can be pleasurable, interesting and can give young people a sense of control.

> ‘It depends on whether it's deliberate or not. if it's intentional then they might be pleasured and interested, however they may be uneasy and disgusted if unintentional’ – eSafety focus group participant, 18
>
> ‘Well, if a child is searching for porn intentionally, they are most likely doing so for arousal’ – eSafety focus group participant, 16
>
> ‘With unintentionally [seeing online pornography] there could be unreasonable guilt but intentionally they could feel in control with their emotions and what they learn’ – eSafety focus group participant, 16

For humour or social status

Several consultation stakeholders referred to anecdotal experiences of children sharing pornography to ‘gross out’ or shock each other, or because they think it is funny. One stakeholder noted this behaviour is common, particularly for boys aged 10-13, and is not unique to sharing pornography – it can include sharing gory or violent videos.

Stakeholders suggested this ties into broader concerns about children’s internet usage and developing norms online. The role of community standards, and enforcement of those standards through effective content moderation, is considered in chapter 11 of this report.

Focus group participants also reflected on how content may be sought out for this purpose.

> ‘Yeah, I think it's quite normalised in children when they aren't educated properly to show their friends pornographic content because they think it's funny or makes them cooler or more mature.’ - eSafety focus group participant, 17
>
> ‘At my school people would share it around for the fun of it to be cool’ – eSafety focus group participant, 18
>
> ‘It is funny to younger kids’ – eSafety focus group participant, 16
>
> ‘Ha yeah definitely, I think I've watched porn about 4 times in my whole life, 3 of them were with a group of people joking around haha’ – eSafety focus group participant, 18

To harass

Consumption of pornography in public places, such as on public transport, in workplaces or at school, has been considered in some reports as sexual harassment of others, particularly girls and young women.[119]

While its use by adults in broader sexual harassment contexts is beyond the scope of this report, stakeholders, particularly those who worked with school-aged children, reported anecdotal examples of children sending explicit content to others for the purposes of bullying and harassment, or watching videos loudly in front of others to make them uncomfortable.[120]

To learn about or explore sexuality

According to research carried out in 2021 by eSafety, almost half of children aged 14–17 (48%) have looked online for sexual health information in the past year, with one in seven (13%) doing so at least weekly.[121]

Several studies and consultation participants suggested that children and young people often seek information about sex through online pornography.

- Children and young people surveyed in 2020 by the South Australian Commissioner for Children and Young People reported using pornography to learn about sex (40% of respondents aged 12 to 14 years, 50% of respondents aged 15 to 18 years and 61% of respondents aged 19 to 22 years), despite also ranking pornography as one of their least trusted sources.[122]
- Several recent Australian and international studies show that LGBTIQ+ children and young people who feel they cannot come out to parents or caregivers rely on more discreet ways to access sexual health information, which can include through pornography. Additionally, pornography may be used to learn about sexual practices not covered in mainstream, school-based education programs.[123]

[119] UK House of Commons Women and Equalities Committee, *Sexual harassment of women and girls in public places: sixth report of session 2017-19*, House of Commons, October 2018. https://committees.parliament.uk/work/6031/sexual-harassment-of-women-and-girls-in-public-places-inquiry/

[120] See Appendix 5.

[121] eSafety Commissioner, *Mind the Gap*, February 2022. https://www.esafety.gov.au/research/mind-gap.

[122] 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. https://www.ccyp.com.au/wp-content/uploads/2022/03/Sex-Education-in-South-Australia.pdf.

[123] A Waling, S Fraser, L Kerr, A Bourne and M Carman, *Young people, sexual literacy and sources of knowledge*, La Trobe University, 2019. https://www.latrobe.edu.au/__data/assets/pdf_file/0011/1072973/Young-People,-Sexual-Literacy-and-Sources-of-Knowledge.pdf; British Board of Film Classification, '*Young people, pornography and age verification*', 2020; https://www.bbfc.co.uk/about-classification/research T Jones and L Hillier, *'Sexuality education school policy for Australian GLBTIQ students'*, Sex Education, 2012, 12(4):437–454; C Fisher et al., '*6th National survey of Australian secondary students and sexual health*', Australian Research Centre in Sex, Health and Society, La Trobe University, 2019. https://www.latrobe.edu.au/__data/assets/pdf_file/0004/1031899/National-Survey-of-Secondary-Students-and-Sexual-Health-2018.pdf; P Byron, A McKee, A Watson, K Litsou and R Ingham, *'Reading for realness: Porn literacies, digital media, and young people'*, Sexuality & Culture, 2021, 25(3):786-805, DOI: 10.1007/s12119-020-09794-6.

The use of online pornography as a supplement to or substitute for school-based sex education is discussed further in chapter 13.

At what age is accessing online pornography harmful?

While the evidence is clear that many children and young people have seen online pornography, the impact on the nature or severity of potential harms due to the age of access is less distinct in the literature.

A report on harmful sexual behaviours in children from ANROWS distinguishes developmentally appropriate behaviours and abnormal/potentially harmful sexual behaviours both on a continuum and classified by developmental stage.[124] It identifies that for children 10-13 and younger, irregular viewing of pornography can be 'concerning sexual behaviour' and chronic pornographic interest can be 'very concerning sexual behaviour' while 'curiosity and seeking information about sexuality' is an 'age-appropriate sexual behaviour' (the report does not discuss the potential intersection between viewing pornography as a means to seek information about sexuality).[125] However, the report says for children 14-18, viewing pornography can be an age-appropriate sexual behaviour.[126]

Several academic stakeholders during our consultation also stated that post-puberty, pornography use could be a normal part of sexual development. There were high levels of agreement across consulted stakeholders that there is a greater potential for harm due to younger exposure – particularly as younger children are less likely to have received relevant education.[127]

Several consultation stakeholders and focus group participants noted the inconsistency between the age of consent to sexual intercourse in Australia (generally 16) and the age at which they are allowed to view sexually explicit material (18). One in two participants in our survey agreed the age of consent (defined as 16 years) should be a factor in the way government approaches restrictions to online pornography. Most (65%) of those surveyed agreed that people under 16 should be restricted from accessing online pornography.

Focus group participants held a range of opinions about when access to online pornography may be harmful for children:

[124] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours,* 2020.
[125] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours,* 2020.
[126] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours,* 2020.
[127] See Appendix 5.

‘I don't think that teenagers under the age of 16 should be viewing pornography’ – eSafety focus group participant, 16

‘16 would be ideal but to be realistic probably 13 or 14’ – eSafety focus group participant, 16

‘Because 16 is the age of consent and they should be considered mature enough to make decisions like this’ – eSafety focus group participant, 16

‘I believe there isn't an appropriate age, and instead whenever the brain has developed enough to understand it, which occurs at different rates for different people’ – eSafety focus group participant, 18

What are the potential impacts for children?

Inquiry submissions and findings

Many submissions to the Inquiry Committee expressed concern about a range of possible consequences associated with children’s access to online pornography and children’s frequent use of online pornography. This included reinforcing harmful gender stereotypes, condoning violence against women, child-on-child sexual abuse and sexually coercive behaviour from young men. The Committee also received evidence suggesting associations between online pornography and broader impacts, ‘such as anxiety about body image, broader mental health issues, reduced academic performance, erectile dysfunction, and systemic issues such as violence against women’.[128]

Limitations of the available literature

Multiple publications which connect pornography to a variety of harms have been criticised as lacking in evidence and relying on biased or moralistic notions of what constitutes harm.[129] For example, some studies have included ‘liberalised attitudes

[128] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, Parliament of Australia, 2020, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report.

[129] R Weitzer, *‘Pornography’s Effects: The Need for Solid Evidence’*, Violence Against Women, 2010, 17(5):666–675, DOI: 10.1177/1077801211407478.

towards sex' as a potential harm from viewing pornography.[130] Studies also apply variable definitions of online pornography.

A 2016 review of pornography literature from the preceding 20 years found that methodological and theoretical shortcomings within the literature limited the ability to draw any causal conclusions about the effects of pornography on adolescents.[131]

Another systematic literature review found that of the articles reviewed, the majority that identified correlations between aspects of sexual health and pornography consumption incorrectly assigned causality to pornography consumption.[132]

A third study which considered research into viewing violent pornography found that direct evidence on how it impacts gender-based violence is inconclusive.[133]

Given the wide range of inter-connected factors which may impact a person's sexual attitudes and behaviours, it is difficult to establish causality. For example, 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, as men with a disposition towards violence against women may be more likely to seek out violent pornography, therefore an association may be correlated and cannot be interpreted as causation.

As such, studies should be compared with care, and any conclusions drawn should consider the limitations of the literature. 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.[134]

[130] M Flood, '*The Harms of Pornography Exposure Among Children and Young People*', Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect, 2009, 18(6):384-400.

[131] J Peter and P Valkenburg, *'Adolescents and Pornography: A Review of 20 Years of Research'*, Journal of Sex Education, 2016, 53(4-5):509-531, DOI: 10.1080/00224499.2016.1143441

[132] A McKee, K Litsou, P Byron and R Ingham, *'The relationship between consumption of pornography and consensual sexual practice: Results of a mixed method systematic review'*, The Canadian Journal of Human Sexuality, 2021, 30(3):387-396, DOI: 10.3138/cjhs.2021-0010.

[133] M Lim, E Carrotte and M Hellard, *'The impact of pornography on gender-based violence, sexual health and well-being: what do we know?*', Journal of Epidemiology and Community Health, 2016, 70(1):3-5, DOI: 10.1136/jech-2015-205453.

[134] For example, in the context of environmental regulators and climate change legal action, see Plan B, *Legal Action: Part 3b Causation*, available at: https://planb.earth/causation/.

Findings from out call for evidence and consultations

Evidence from academic literature indicates there are correlations between viewing pornography and the negative impacts explored below.

However, there is conflicting evidence about the association and extent of both individual and societal harms to children from accessing online pornography.

While it can be difficult to isolate online pornography from other contributing factors – for example, harmful views on gender which are pervasive across society more broadly – it is nevertheless important to consider its potential role and impacts. Importantly, the prevalence and pervasiveness of online pornography has been identified as a 'serious concern in addressing the drivers of violence against women and children' in Australia. [135]

Potential impacts

Gender-based violence and harmful views about sex and gender

The scripts and depictions within mainstream pornography can both reflect and contribute to a culture that normalises, condones, and minimises gender-based violence.[136]

According to Our Watch, violence against women and children is underpinned by four key drivers that consistently predict or 'drive' violence against women and explain its gendered patterns and dynamics.[137] They are:

- Rigid gender roles and stereotyped constructions of masculinity and femininity
- Men's control of decision-making and limits to women's independence in public and private life
- Condoning of violence against women
- Male peer relations that emphasise aggression and disrespect towards women[138]

Studies show that mainstream pornography commonly perpetuates and upholds these drivers.[139] Mainstream online pornography is noted for containing and normalising depictions of sexual violence and degrading sexual scripts about women, often based on racist and sexist

[135] Commonwealth of Australia, *National Plan to End Violence against Women and Children 2022-2032*, Department of Social Services, 2022. https://www.dss.gov.au/ending-violence.

[136] Vera-Gray et al., *'Sexual violence as a sexual script in mainstream online pornography'*, 2021.

[137] OurWatch, *Change the story: A shared framework for the primary prevention of violence against women in Australia (second edition)*, 2021. https://media-cdn.ourwatch.org.au/wp-content/uploads/sites/2/2021/11/18101814/Change-the-story-Our-Watch-AA.pdf.

[138] OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020.

[139] Coy and Tyler, 2022; R Mikorski and D Szymanski, *'Masculine norms, peer group, pornography, Facebook, and men's sexual objectification of women'*, Psychology of Men & Masculinity, 2017, 18(4):257-267, DOI: 10.1037/men0000058; OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020.

stereotypes and harmful gender norms. This can have negative impacts for groups and society more broadly by circulating a view of women as subordinate, especially women of colour.[140] Mainstream pornography provides a 'conducive context' to gender-based violence and gender inequality.[141]

National Plan to End Violence against Women and Children 2022-2032

The *National Plan to End Violence against Women and Children 2022-2032* (National Plan) is Australia's overarching policy framework guiding how Australia addresses gender-based violence.

The National Plan draws a connection between pornography and gender-based violence, noting that the physical and verbal aggression towards women, male dominance and female submission, and non-consensual behaviours, and the sexist, misogynistic and degrading views about women often depicted in online pornography make it a serious concern and a focus area in addressing the drivers of violence against women and children.[142]

As the National Plan acknowledges, the relationship between pornography and gender-based violence is complex, but increasingly, correlations are being made between pornography use and less progressive attitudes about gender roles, a belief that women are sex objects, and the acceptance of harmful myths about rape and sexual consent.[143]

This is supported by research highlighting that mainstream pornography often:

- eroticises gender inequality, including through male sexual aggression, unequal power dynamics, a lack of consent, sexual violence, and themes of incest.[144]
- normalises women's sexual abuse, including through the common promotion and featuring of acts such as painful anal penetration, slapping and choking, aggressive

[140] Vera-Gray et al., *'Sexual violence as a sexual script in mainstream online pornography',* 2021; W DeKeseredy and A Hall-Sanchez, *'Thinking critically about contemporary adult pornography and woman abuse'*, in W DeKeseredy and M Dragiewicz (eds), Routledge Handbook of Critical Criminology, Routledge, 2018.

[141] N Jovanovski and M Tyler, '*Pornography encouraged me to belittle women: A thematic analysis of men's reflections on violence against women and ceasing pornography use',* Violence Against Women, 2022, DOI: 10.1177/10778012221125502.

[142] Commonwealth of Australia, *National Plan to End Violence against Women and Children 2022-2032*, 2022.

[143] Commonwealth of Australia, *National Plan to End Violence against Women and Children 2022-2032*, 2022.

[144] Vera-Gray et al., *'Sexual violence as a sexual script in mainstream online pornography',* 2021; M Flood and S Burrell, *'Engaging men and boys in the primary prevention of sexual violence'*, in M Horvath & J Brown (eds), Rape: Challenging contemporary thinking – 10 years on (2nd ed.), Routledge, 2022.

deep throat causing women to cry and vomit, 'ass-to-mouth', spitting and urinating on women.[145]

- depicts women accepting and welcoming abuse.[146]
- perpetuates heteronormative sexual scripts, involving aggression towards and submission of women,[147] and rarely portrays negative repercussions due to aggression or violence.[148]
- perpetuates racist sexual scripts, including portrayals of stereotypes that depict Asian women as passive, servile and childlike possessions for white colonial consumption, and portrayals of women of colour as deviant, hypersexual and animal-like.[149]
- both fetishises and excludes differences in a way that reflects racism, homophobia, transphobia and ableism.[150]
- commodifies women's abuse, with the eroticisation of gender inequality and victimisation of women featuring in the titles of or otherwise noted as the 'selling point' in many videos.[151]
- promotes stereotyped gender roles and constructions of masculinity and femininity in ways that may limit girls' and women's equal and free participation in public and private life.[152]
- normalises the objectification and dehumanisation of women, legitimises male entitlement, prioritises heterosexist ideas on male sexuality and centres the male gaze.[153]

[145] W DeKeseredy and A Hall-Sanchez, *'Adult pornography and violence against women in the Heartland: Results from a rural Southeast Ohio study',* Violence Against Women, 2017, 23(7):830-849; G Dines, '*Pornland: How porn has hijacked our sexuality',* Beacon Press, Boston, 2010; R Saunders, *Bodies of work: The labour of sex in the digital age,* Springer, 2020; N Fritz, V Malic, B Paul and Y Zhou, *'A descriptive analysis of the types, targets, and relative frequency of aggression in mainstream pornography'*, Archives of Sexual Behaviour, 2020, 49(1):3041–3053, DOI: 10.1007/s10508-020-01773-0

[146] R Whisnant, *'Pornography, humiliation, and consent'*, Sexualization, Media, & Society, 2016, 2(3), DOI:1177/2374623816662876

[147] R Carrotte, A Davis, and M Lim, *'Sexual behaviours and violence in pornography: Systematic review and narrative synthesis of video content analyses'*, Journal of Medical Internet Research, 2020, 22(5), DOI: 10.2196/16702.

[148] Fritz et al., 2020.

[149] M Donevan, *'If pornography is sex education, what does it teach?'*, in M Kiraly and M Tyler (eds), Freedom Fallacy: The Limits of Liberal Feminism, Connor Court Publishing, Ballarat, Australia, 2015.

[150] J Lavigne, *'Autopornography and the struggle for the recognition of a sexual subjectivity: a theoretical analysis from Loree Erickson's testimony in The Feminist Porn Book'*, Feminist Media Studies, 2017, 17(5):790-803.

[151] Saunders, 2020.

[152] S Amankaviciute, H Pringle and M Zalnieriute, '*The role of sexist abuse and objectification in women's activism'*, 2021, DOI: 10.2139/ssrn.3943791; H Pringle, M Zalnieriute, & S Amankaviciute, *'Addressing harassment as systemic discrimination: Realising CEDAW's promise of substantive equality'*, Submission to Inquiry into the Sex Discrimination and Fair Work (Respect at Work) Amendment Bill, 2021.

[153] Flood and Burrell, 2022.

Online pornography of this nature is often immediately available on the homepage of free and popular tube sites.[154] Researchers have also noted that these scripts may also shape acts and depictions in LGBTIQ+ pornography, with aggression and stereotyped gender roles and constructions of masculinity and femininity also featuring in same-sex pornography videos.[155]

There is an emerging body of research looking at how women's experiences of intimate partner violence may be influenced by online pornography. Studies from the US and Australia both reflect the use of pornography as a kind of 'manual' in the sexual abuse of women by their intimate partners, with perpetrators of violence replicating what they have seen in pornography.[156] This is echoed by researchers and practitioners uncovering the links between various facets of family and domestic violence and pornography – and also including the ways pornography is used against children of male pornography consumers in family violence. This includes research that notes male consumers exposing their children to pornography when a female partner is absent.[157]

It is important to acknowledge attempts to produce alternative pornographies through 'niche' genres, such as those considered feminist, ethical and/or female-produced pornography. Some female performers and producers have found this provides opportunities for liberated forms of female sexual expression and more equitable on-set conditions. Some studies have found examples of pornography which have been promoted as feminist or ethical but instead reproduce the practices of violence against women and coercion found in mainstream pornography.[158]

Notably, in our consultations, stakeholders from the adult industry expressed concern that sexually explicit material is viewed as a monolith and current dialogue on the topic focuses disproportionately on content which depicts misogyny, racism and implied or actual non-consent. They believe this misrepresents the diversity of bodies, acts and stories represented across the industry.

[154] M Klaassen and J Peter, *'Gender (in)equality in internet pornography: A content analysis of popular pornographic internet videos',* The Journal of Sex Research, 2015, 52(7):721-735, DOI:10.1080/00224499.2014.976781; Y Zhou, T Liu, Y Yan and B Paul, *'Pornography use, two forms of dehumanization, and sexual aggression: Attitudes vs. behaviours'*, Journal of Sex & Marital Therapy, 2021, 47(6):571-590, DOI: 10.1080/0092623X.2021.1923598.

[155] K Seida and E Shor, *'Aggression and pleasure in opposite-sex and same-sex mainstream online pornography: A comparative content analysis of dyadic scenes',* The Journal of Sex Research, 2021, 58(3):292-304, DOI: 10.1080/00224499.2019.1696275.

[156] DeKeseredy and Hall-Sanchez, 2017; L Tarzia and M Tyler, *'Recognizing connections between intimate partner sexual violence and pornography',* Violence Against Women, 2021, 27(14):2687–2708, DOI:10.1177/1077801220971352.

[157] W DeKeseredy, *Domestic violence: The contribution of contemporary pornography*, Culture Reframed, December 2022., available at: https://culturereframed.org/domestic-violence-the-contribution-of-contemporary-pornography/; J Johnson, A Bridges, M Ezzell, C Sun, S Aadahl, G Amabile and C Leahy, *'Understanding a context of risk: Pornography and child sexual abuse',* 2022, DOI: 10.31235/osf.io/kf4uv.

[158] R Saunders, '*Grey, gonzo and the grotesque: the legacy of porn star Sasha Grey',* Porn Studies, 2018, 5(4):363-379, DOI: 10.1080/23268743.2018.1505544; R Whisnant, *'But what about feminist porn? Examining the work of Tristan Taormino'*, Sexualization, Media, & Society, 2016, 2(2).

Harmful views amongst children

There is evidence that seeing pornography may be associated with children having harmful views about sex and gender. There are ongoing debates about the effects media content has on viewers, with some theories suggesting media content can activate 'scripts' for behaviour[159] and others arguing that while there may be a correlation between content consumed and behaviour, there is no causal link.[160]

Most participants in our survey with young people thought online pornography negatively impacted on children's and young people's understandings of consent (74%), ideas about intimate relationships (76%), expectations of sex (76%), and views on gender stereotypes (64%).

> 'I believe it is something that people can view just like any show or movie however when it begins to affect people expectations/thoughts negatively then its bad' – eSafety focus group participant, 16
>
> 'Sometimes positions/activities turn people off or even hurt those involved, which pornography avoids and assumes that every sexual activity is enjoyed by both people' – eSafety focus group participant, 18

Focus group participants discussed the harmful stereotypes of male dominance and female objectification that could arise if some of the content depicted in online pornography was understood by viewers as a common and acceptable sexual practice.

> 'Well, if someone's first experience of sex is online pornography, it can be incredibly harmful. They might think certain things that happen in porn are normal, which could result in harming others, or doing things without consent, just because they want something' – eSafety focus group participant, 16
>
> 'I think a lot of porn is fetishised which can create harmful stereotypes' – eSafety focus group participant, 18

First Nations community front line workers who spoke with eSafety in 2022 shared how they had observed children in their community, and in particular young boys, watching online pornography on their phones. They shared their concern that this was impacting the children's understanding of respectful relationships and could be normalising violent sexual behaviours.[161]

[159] P Wright and M Funk, *'Pornography consumption and opposition to affirmative action for women: A prospective study'*, Psychology of Women Quarterly, 2014, 38(2):208-221, DOI:10.1177/0361684313498853.
[160] A McKee, *'The importance of entertainment for sexuality education'*, Sex Education, 2012, 12(5):499-509, DOI: 10.1080/14681811.2011.627727.
[161] First Nation eSafety research, unpublished.

OurWatch's study with 15–20-year-olds found links between viewing pornography and a belief in rigid gender roles: the view that men should be 'in charge', attitudes condoning violence against women, and the condoning of male peer relationships that are disrespectful towards women.[162]

Some international studies have found similar conclusions:

- A UK literature review found there is evidence to suggest young people appear to become desensitised to the content of pornography over time and that pornography can influence attitudes such as the acceptance of sexual aggression towards women and victim-blaming attitudes.[163]
- In a five-country European study of participants aged 14-17, boys' engagement in sexual coercion and abuse was significantly associated with regular viewing of online pornography.[164]
- A study with 16–26-year-olds in Norway also found that exposure to pornography was moderately associated with being harassed and harassing others.[165]

Some studies found nuance in the types of views associated with seeing pornography:

- A study with 16–26-year-olds in Norway found that exposure to pornography was not associated with coercive attitudes but was weakly associated with classical sexism in males.[166]
- A longitudinal study with high schoolers in the US found that encountering sexually explicit media was not associated with gender role attitudes.[167]
- A large study of adults aged 18-89 in the US found that viewing pornography was associated over time with an increase in gender role attitudes towards women in older adults (over 45) but not in younger adults.[168] However, some scholars have called into question how gendered harms would manifest for adults but young people would remain unaffected.[169]

[162] OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020.
[163] Ofsted, *Review of sexual abuse in schools and colleges*, UK Government, 2021. https://www.gov.uk/government/publications/review-of-sexual-abuse-in-schools-and-colleges/review-of-sexual-abuse-in-schools-and-colleges.
[164] N Stanley, C Barter, M Wood, N Aghtaie, C Larkins, A Lanau and C Överlien, *'Pornography, sexual coercion and abuse and sexting in young people's intimate relationships: A European study'*, Journal of Interpersonal Violence, 2018, 33(19):2919-2944. DOI: 10.1177/088626051663320.
[165] L Kennair and M Bendixen, *'Sociosexuality as predictor of sexual harassment and coercion in female and male high school students',* Evolution and Human Behaviour, 2012, 33(5):479-490, DOI: 10.1016/j.evolhumbehav.2012.01.001.
[166] Kennair and Bendixen, 2012.
[167] J Brown and K L'Engle *'X-rated: Sexual attitudes and behaviours associated with US early adolescents' exposure to sexually explicit media',* Communication Research, 2009, 36(1):129-151, DOI: 10.1177/0093650208326465.
[168] P Wright and S Bae, '*A national prospective study of pornography consumption and gendered attitudes toward women'*, Sexuality & Culture, 2015, 19(3):444-463.
[169] Coy and Tyler, 2022.

Sexual aggression and harm

Evidence cited in submissions to eSafety indicates an association between seeing online pornography and either engaging in sexual harm or being a victim/survivor of sexual harm. However, this evidence also indicates there are usually additional factors at play.

A 2016 literature review found that studies tended to show a relationship between adolescents' viewing pornography and a higher likelihood of carrying out and experiencing sexual aggression. There was evidence of a stronger relationship between watching pornography and engaging in sexual aggression for boys, and a stronger relationship between watching pornography and experiencing sexual aggression for girls.[170]

Engaging in harmful sexual behaviours (including peer-on-peer abuse)

The association between seeing pornography and engaging in harmful sexual behaviours is often found to be moderated by factors such as attitudes towards sex among children and young people, and levels of hostile masculinity in adults.[171]

The report from ANROWS notes at present, there is limited understanding and a lack of research on the association between children and young people viewing and engaging with online pornography and demonstrating or engaging in harmful sexual behaviour.

In addition to pornography, the literature has identified several factors which are often associated with young people engaging in harmful sexual behaviours. This includes being male, histories of trauma (such as neglect and abuse), learning, cognitive and intellectual disabilities, family conflict and dysfunction, parental alcohol and substance misuse, and placement and care instability. These factors should not be considered casual but considered a part of the overall circumstances in which this behaviour occurs.[172]

The report also notes that the research to date has focused on individual and interpersonal factors. Challenges remain in identifying and assessing factors at a community and socio-cultural level.

[170] Peter and Valkenburg, 2016.

[171] Y Rodríguez-Castro et al., R Martínez-Román, P Alonso-Ruido, A Adá-Lameiras and M Carrera-Fernández, *'Intimate partner cyberstalking, sexism, pornography, and sexting in adolescents: New challenges for sex education',* International Journal of Environmental Research and Public Health, 2021, 18(4):2181; M Stoilova, S Livingstone and R Khazbak, *Investigating risks and opportunities for children in a digital world: A rapid review of the evidence on children's internet use and outcomes,* UNICEF, 2021, available at: https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf.

[172] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours*, 2020.

One Australian study from 2014 suggests there may be a link between 7–18-year-olds who were in treatment for engaging in harmful sexual behaviours and seeing pornography at a young age. However, the study also notes more research is needed in this area.[173]

Violent behaviour and violence in pornography

There are studies which have investigated the type of pornography young people encounter and have suggested there may be a link between violent pornography (as opposed to non-violent pornography) and engaging in harmful sexual behaviours.

A US-based study conducted in six ‘waves’ between 2006 and 2012, found that seeing violent pornography between the ages of 10 to 21 was associated with carrying out sexual harassment, sexual assault and coercive sex. The study did not find the same associations for those who had seen non-violent pornography.[174] However, other factors were also found to contribute to the likelihood of engaging in harmful sexual behaviour such as broader aggressive behaviour, exposure to caregiver’s violent romantic partnerships, prior attitudes accepting violence in relationships, and the perception that young people are expected to have sex.

A separate 2019 study with grade 10 students in the US found that those who had seen violent pornography were more likely to engage in teen dating violence (1.5 times more likely for girls, 3 times more likely for boys).[175] Boys who viewed violent pornography were also found to be twice as likely to experience physical and sexual teen dating violence.

Other studies found correlations between the type of content consumed and violent behaviours. For example, on study found that children who consumed violent sexually explicit material were almost six times more likely than those who did not consume such content to engage in sexually aggressive behaviour.[176]

Some academics have found that many studies considering aggression and violence in pornography fail to differentiate between consensual aggression and non-consensual aggression.[177]

[173] L Etheredge and J Lemon, *Pornography, problem sexual behaviour and sibling on sibling sexual violence*, Submission to the Royal Commission into Family Violence, Victoria, 2015, SUBM.0220.001.0001.

[174] M Ybarra and R Thompson*, ‘Predicting the emergence of sexual violence in adolescence*,’ Prevention Science, 2018, 19(4):403-415, DOI: 10.1007/s11121-017-0810-4.

[175] W Rostad, D Gittins-Stone, C Huntington, C Rizzo, D Pearman and L Orchowski, *‘The association between exposure to violent pornography and teen dating violence in grade 10 high school students’*, Archives of Sexual Behaviour, 2019, 48(7):2137-2147, DOI: 10.1007/s10508-019-1435-4.

[176] Ybarra, M. L., Mitchell, K. J., Hamburger, M., Diener-West, M., & Leaf, P. J. 2011. ‘*X-rated material and perpetration of sexually aggressive behavior among children and adolescents: Is there a link? Aggressive Behavio’*r, 37(1), 1-18. DOI: 10.1002/ab.20367 in M Proeve, C Malvaso and P DelFabbro, *Evidence and frameworks for understanding perpetrators of institutional child sexual abuse,* Royal Commission into Institutional Responses to Child Sexual Abuse, 2016, p 46 https://www.childabuseroyalcommission.gov.au/research

[177] K Litsou, P Byron, A McKee and R Ingham, *‘Learning from pornography: Results of a mixed methods systematic review’*, Sex Education, 2021, 21(2):236-252, DOI: 10.1080/14681811.2020.1786362; A McKee*, ‘The importance of entertainment for sexuality education’*, Sex Education, 2012, 12(5):499-509, DOI: 10.1080/14681811.2011.627727.

In a 2020 ANROWS survey of professionals working with young people that display sexually abusive behaviours, 40% (n=24) of respondents identified exposure to pornography as one of the top three common risk factors for their client base.[178] Similarly, submissions to the *Royal Commission into Institutional Responses to Child Sexual Abuse* provided examples of services treating children who had previously harmed others through re-enactments of sexual activities they had seen in pornography.[179]

This was also discussed during eSafety's consultations with researchers and clinical therapists for young people that had been court sanctioned for sexual offences. These stakeholders noted that identifying a causal link between pornography consumption and harmful sexual behaviours is not straightforward and there is substantial complexity in the way harmful behaviours present among young people. They advised that the role, if any, of online pornography in influencing their clients was assessed on a case-by-case basis.

Pornography educating young people in harmful, unsafe or unrealistic practices

> 'I think porn can be incredibly harmful but also incredibly helpful, it's a mixed bag depending on who you are and your own situation. You can use it to explore yourself, but it can also hinder you and give unrealistic views and opinions on real matters, plus the industry can be terrible to women and children' – eSafety focus group participant, 17

Online pornography is sometimes a source of information for children and young people about sex and as well as providing an avenue for sexual exploration and expression. It can create the potential for harm where sex is portrayed as aggressive, violent, or does not depict important safety and consent practices.[180] For example, a 2018 study among 14-17-year-olds in five European countries concluded pornography had the potential to inform sexually coercive and abusive behaviour in young men.[181] A 2020 study found that many 11–16-year-olds in the UK get ideas about types of sex they want to try from online pornography, and that pornography has given some of them ideas about how women should behave during sex. However, the authors note this data cannot tell us the concepts participants assimilate from pornography and whether they are about safe sex or potentially harmful practices.[182]

In our consultations, law enforcement stakeholders identified increasing numbers of teenage girls presenting to hospital for medical treatment from injuries sustained through sexual activity

[178] Quadara et al., *Good practice in delivering and evaluating interventions for young people with harmful sexual behaviours*, 2020.

[179] Royal Commission into Institutional Responses to Child Sexual Abuse, 2017. https://www.childabuseroyalcommission.gov.au/document-library

[180] R Saunders, 2020.

[181] N Stanley et al., 2018.

[182] E Martellozzo, A Monaghan, J Davidson and J Adler, *'Researching the affects that online pornography has on U.K. adolescents aged 11 to 16'*, 2020, SAGE Open, 10(1), DOI: 10.1177/215824401989946.

that may be influenced by online pornography. However, limits to data sharing practices between law enforcement and health professionals create challenges for drawing conclusions. For example, it is unclear whether harms stem from young people not being aware of safe practices for certain sexual activities, whether activities are coerced or non-consensual, or a combination of both. Academic stakeholders expressed that whole categories of sexual activity should not be deemed inherently harmful merely because they carry a risk of physical harm.

Choking or sexual strangulation

Choking, or sexual strangulation, was raised as a particular concern by some stakeholders during consultation. In a 2020 survey of US undergraduate students, 58% of women, 26% of men, and 45% of gender expansive students had been choked during sex.[183]

In qualitative interviews with US college students aged 18-33, participants described first becoming aware of choking in high school or college, with 6 out of 24 participants reporting learning about choking from pornography. Most reported that they had seen the act in pornography at some point. Many participants said pornography played a role in their partner choking them. [184]

However, the study authors note that pornography is not the only place where adolescents and young people learn about choking. Participants described seeing or reading about choking within a diverse range of media, including 'magazines, social media, mainstream television and movies, and popular erotica.'

This is an emerging area of research and will be the subject of an upcoming public awareness campaign from *It's Time We Talked.* Understanding emerging trends in online pornography and in children's and young people's behaviour is important to make sure relevant educational measures are effective and targeted.

Research in 2018 found that young men aged 16-18 years in England lacked awareness on how to make anal sex comfortable and pleasurable for women being penetrated and suggested this could have resulted from using pornography as sex education. The study also argued that a more fundamental health risk among children is an absence of considering consent, noting this

[183] D Herbenick, L Guerra-Reyes, C Patterson, Y Rosenstock Gonzalez, C Wager and N Zounlome *'It was scary, but then it was kind of exciting': Young women's experiences with choking during sex'*, Archives of Sexual Behaviour, 2022, 51(2):1103-1123, DOI: 10.1007/s10508-021-02049-x.

[184] D Herbenick et al., 2022.

is a long-standing concern about sexual behaviours that may or may not be associated with viewing online pornography.[185]

In a 2018 New Zealand study with participants aged 14-17, some reported they had used pornography to figure out what feels good for them and their partners, while others were concerned that using pornography as a guide could lead to negative experiences as they begin to explore sex. About one third of participants had either tried something with a partner they had learned from seeing in pornography, or their partner had tried something with them.[186]

Some studies show young people are aware that pornography is not a good source of sex education.[187] 43% of respondents to our survey thought online pornography's effect on young people learning about sex and exploring their sexuality was negative or very negative.[188]

While most pornography may not provide sound advice about consent and safer sex practices, a systematic review published in 2020 found that pornography can offer viewers (especially gay males), 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.[189]

Research from the South Australian Commissioner for Children and Young People, found 33.5% of LGBTQA+ students in South Australian secondary schools reported never having LGBTQA+ people mentioned in a supportive or inclusive way during their relationship and sex health education.[190]

In our research, LGB+ participants were significantly more likely to think online pornography had some positive effect on young people learning about sex and exploring their sexuality than heterosexual participants (60% vs. 48%).[191]

Unrealistic depictions and expectations

Research with young people aged 14-17 from the Office of Film and Literature Classification in New Zealand found that most participants felt pornography was not a realistic portrayal of sex or relationships. This reflected the Office's 2018 survey, where young people 'unprompted and irrespective of gender, age or background, raised the 'unrealistic', 'fake' or 'false' nature of porn

[185] C Marston, *'Pornography and young people's health: Evidence from the UK sixteen18 project',* Porn Studies, 2018, 5(2):1-4, DOI: 10.1080/23268743.2018.1434153.
[186] Henry and Talbot, 2019.
[187] OurWatch, *Pornography, young people and preventing violence against women background paper*, 2020; K Litsou, P Byron, A McKee and R Ingham, *'Learning from pornography: Results of a mixed methods systematic review',* Sex Education, 2021, 21(2):236-252, DOI: 10.1080/14681811.2020.1786362.
[188] eSafety research, forthcoming.
[189] Litsou et al, *'Learning from pornography: Results of a mixed methods systematic review'*, 2021.
[190] 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.
[191] eSafety research, forthcoming.

and the impact this could have on people.' This was the most cited negative impact of online pornography in the study.[192]

Some academics we spoke to during consultations challenged the assumption that pornography is always unrealistic, noting that studies which characterise pornography in this way often describe pleasure derived from any acts other than heterosexual, penetrative sex as 'unrealistic'. One academic noted from their own research that many young people understand pornography is not real but have difficulty in identifying or articulating which specific aspects are unrealistic.[193]

When raised in our focus groups, some participants explained how they thought pornography could be unrealistic:

> 'Sometimes positions/activities turn people off or even hurt those involved, which pornography avoids and assumes that every sexual activity is enjoyed by both people' – eSafety focus group participant, 18
>
> 'That sex is focused on men finishing and not providing the woman any pleasure' – eSafety focus group participant, 16

Almost three in four (73%) 16-18-year-olds in our survey thought education and information to help young people distinguish pornography from actual sex would be helpful to manage the negative impacts of online pornography. Teaching young people to distinguish pornography from real-life sex was also described as being important by some focus group participants.

> 'I think that learning how to distinguish porn from reality would be a good start' – eSafety focus group participant, 18
>
> '...to realise that porn most times is just like any film or show and that it's not reality' – eSafety focus group participant, 16

Educational measures to address this need are discussed in chapter 13.

Encouraging sexually risky behaviour

Many studies inquire into the links between seeing pornography and engaging in sexually risky behaviour. However, there are some limitations to the findings, including how 'sexual risk' is defined across each study.

[192] NZ Classification Office, *Growing up with Porn* report, NZ Classification Office Te Mana Whaakatu, April 2020. https://www.classificationoffice.govt.nz/resources/research/growing-up-with-porn/.
[193] See Appendix 5.

In consultations, academic stakeholders also expressed concern about studies which characterised sexual adventurousness, or non-heteronormative sexual practices, as inherently harmful or risky behaviour.

Research cited in submissions indicates there may be associations between seeing online pornography and engaging in sex casually, without protection, or at a younger age. Notably, these associations are not direct causal relationships.

- A rapid evidence review conducted for UNICEF in 2021 found that across the eighteen studies reviewed, children under 18 who view pornography online have been found to be more likely to have experiences of 'risky sexual activities.' In this study, this term included casual sex, sexual sensation seeking and exposure to unwanted sexual solicitation. [194] The report notes that several factors (internet-related and not) mediate this relationship.
- A 2013 UK rapid evidence assessment found that encountering pornography was associated with children and young people subsequently engaging in risky sexual behaviours. Risks identified in this study included commencing sexual practices at a younger age, engaging in unprotected anal or oral sex, and the involvement of drugs or alcohol in sex.[195] However, the study notes much of the research considered found this is cross-sectional and/or correlational with online pornography and therefore causal relationships cannot be established.
- In contrast, a 2017 study with Victorians aged 15-29 found there was no association between watching pornography frequently (monthly, weekly or daily) and greater sexually risky behaviour.[196] The same study found an association between younger ages for first sexual experiences and younger pornography viewing, but no correlation between younger ages for viewing pornography and sexually risky behaviour. In this paper, sexual risk referred to participants' reporting of sexual intercourse without using condoms in the past 12 months.

General distress and discomfort

Evidence cited in submissions to eSafety indicated children can feel distressed and concerned when they see online pornography.

Focus groups participants typically felt very negatively about unintentional encounters with online pornography. For many participants, the experience of unintentionally encountering

[194] Stoilova et al., *Investigating risks and opportunities for children in a digital world: A rapid review of the evidence on children's internet use and outcomes,* 2021.

[195] M Horvath et al., *'Basically ... Porn is everywhere': A rapid evidence assessment on the effects that access and exposure to pornography has on children and young people*, 2013.

[196] Lim et al., *Young Australians' use of pornography and associations with sexual risk behaviours.*

online pornography was unwelcome and unwanted. They described the emotional experience of unintentionally seeing online pornography as intrusive, uncomfortable and disempowering.

> 'Depends on the intentions. Some people would feel very uncomfortable if they come across it accidently, but on the other hand feel pleasure or interest when looking for it' – eSafety focus group participant, 18
>
> 'It's different when we see it by force, if we search it up, we are prepared for it but when we stumble across it its gross and unwanted' – eSafety focus group participant, 17
>
> '...takes away the choice to access explicit content, as it is pretty much shoved in your face' – eSafety focus group participant, 18

A New Zealand study found that 55% of 14-17-year-olds who had seen pornography in the last six months said they had 'sometimes' seen things that disturbed them, and a further 17% said they had 'often' seen something that disturbed them. Another 17% had not seen something that disturbed them, and the remainder said they were unsure or preferred not to say.[197]

Academic stakeholders who participated in our consultation said young people have natural interests and curiosities that can be explored through pornography in a healthy and developmentally appropriate way. However, young people who have not received any education or support may be more likely to experience harm.[198]

Shame and stigma

Some stakeholders and researchers have pointed to the negative impacts of interventions and messaging which stigmatises the viewing of online pornography and makes young people feel ashamed of their interest in or experiences with it.

Some academic stakeholders suggested the source of harm for pre-pubescent access is often the shame and hostile reactions of trusted adults, rather than a response to the material itself.[199] Similarly, a study of submissions to sexual health websites catering to teens in Finland found that discourses around pornography as harmful, and the subsequent shame and anxiety young people feel when seeing it, are more concerning to young people than the pornography itself.[200]

[197] Henry and Talbot, 2019.
[198] See Appendix 5.
[199] McKee et al., 2010; 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*', Sex Education, 2016, 16(2):130-142, DOI:10.1080/14681811.2015.1080158; See Appendix 5.
[200] Spišák, 2016.

In a 2023 study of US teenagers aged 13-17, half of respondents said they ‘feel guilty or ashamed after watching online porn.’ This was especially pronounced among respondents who reported their only exposure to pornography had been accidental (67%).[201]

Our survey findings indicated that four out of five participants thought feeling embarrassed about the topic (80%) and being judged or shamed (77%) were the main reasons young people may not seek help to manage the negative impacts of online pornography.

> ‘Even though its more normalised I feel like there's still a bit of a stigma around it, which there shouldn't be’ – eSafety focus group participant, 18

Normalisation of content and viewing habits

Some focus group participants suggested their age group was desensitised to pornography because it has become so normal to see it online. Our survey data indicated about one in three (35%) participants who had unintentional encounters with online pornography simply ignored it. This aligns with past research which suggested that young people’s perceptions of, and response towards, online pornography may shift with time, in that they may become habituated or desensitised to explicit content.[202]

> ‘Porn isn’t anything to gasp at as most of us know what it is and how to find it. Its already been normalised between teenagers at least’ (sic) – eSafety focus group participant, 17
>
> ‘A lot of my friends (Girls btw, she/her for me too lol) get uncomfortable if privately shared, but if we come across it on the internet, we have just learnt to ignore it, refrain from watching’ – eSafety focus group participant, 18

Our consultation with Australian education stakeholders revealed an observed pattern of students viewing pornography from increasingly younger ages, with the use of pornography being normalised by the time students reach secondary school.[203]

Stakeholders in our consultations also referenced instances of pre-school aged children ‘acting out what they have seen and experienced, sexually abusing others in schools, kindergartens and childcare settings’.[204]

[201] M Robb and S Mann, *Teens and pornography*, Common Sense Media, 2022. https://www.commonsensemedia.org/research/teens-and-pornography.

[202] E Martellozzo, A Monaghan, J Adler, J Davidson, R Leyva and M Horvath, *‘I wasn't sure it was normal to watch it’*, 2017, doi:10.6084/m9.figshare.3382393; K Daneback, A Ševčíková and Ježek, *‘Exposure to online sexual materials in adolescence and desensitization to sexual content,’* Sexologies, 2018, 27(3):e71-e76, DOI: 10.1016/j.sexol.2018.04.001.

[203] See Appendix 5.

[204] See Appendix 5.

A review of sexual abuse in schools and colleges in the UK found there is insufficient evidence to demonstrate that viewing pornography leads directly to harmful sexual behaviours. However, there is evidence to suggest children appear to become desensitised to its content over time.[205]

Addiction and sexual dysfunction

Some literature suggests pornography use can become addictive. This was also raised as a concern by some stakeholders during our consultation process.[206] The concept of pornography addiction is a contested one, with researchers disagreeing over whether excessive use of visual sexual stimuli can be classified as a behavioural addiction, an impulse control disorder, or something else altogether. Each of these categories has specific and overlapping classificatory criteria and imply different brain activity effects and treatment options. Importantly, while there is debate over how to classify excessive or disruptive pornography use, most researchers agree that some individuals can and do experience their pornography use as problematic.[207]

As such, 'hypersexual behaviour' (the umbrella term under which problematic online pornography use falls) is often considered to be either an impulse control disorder or a behavioural addiction.[208] Those who argue that pornography can be an addiction often draw on substance addiction models, which rely on changes in the brain to prove addiction.[209] There is evidence which shows that watching pornography can produce similar reactions in the brain to drug use.[210] Specifically, one study found that parts of the brain associated with 'craving' were more highly activated among people with compulsive sexual behaviours when shown visual sexual stimuli, than those without those behaviours.[211] However, another evidence review, published in the same year, claimed that engaging in visual sexual stimuli had no different effect on the brain than any other content 'liked' by individuals.[212] Additionally, some contend that the brain's reaction to sexual pleasure experienced while viewing pornography sets up a 'reward' association between pleasure and pornography that can lead to addiction.[213]

[205] Ofsted, *Review of sexual abuse in schools and colleges*, UK 2021

[206] D Mead and M Sharpe, *Research into children's consumption of pornography,* Submission to the Australian Senate Inquiry 'Harm being done to Australian children through access to pornography on the Internet', 2016.

[207] R De Alarcón, J de la Iglesia and N Casado, *'Online porn addiction: What we know and what we don't—A systematic review'*, Journal of Clinical Medicine, 2019, 8(1):E91, DOI: 10.3390/jcm8010091; D Ley, N Prause and P Finn*, 'The emperor has no clothes: A review of the 'pornography addiction' model'*, Current Sexual Health Reports, 2014, 6(2):94-105; A Van Rooij and N Prause, *'A critical review of 'Internet addiction' criteria with suggestions for the future',* Journal of Behavioural Addictions*,* 2014, 3(4):203-213, DOI: 10.1556/JBA.3.2014.4.1.

[208] De Alarcón et al., 2019.

[209] Ley et al., 2014.

[210] D Mead, *'The Risks Young People Face as Porn Consumers',* Addicta, The Turkish Journal of Addictions, 2016, 3(3), DOI: 10.15805/addicta.2016.3.0109; D Mead and M Sharpe*, 'Aligning the 'Manifesto for a European research network into problematic usage of the Internet' with the diverse needs of the professional and consumer communities affected by problematic use of pornography'*, International Journal of Environmental Research and Public Health*,* 2020, 17(10):3462, DOI: 10.3390/ijerph17103462.

[211] V Voon et al., '*Neural correlates of sexual cue reactivity in individuals with and without compulsive sexual behaviours*', PloS One, 2014, 9(7): e102419, DOI: 10.1371/journal.pone.0102419.

[212] Ley et al., 2014.

[213] Mead and Sharpe, 2020.

In contrast, understandings of online pornography as addictive are critiqued as based on insufficient evidence and possible bias. Some researchers argue that the term 'addiction' is used as a moral judgement which determines certain behaviours as problematic based on their social acceptability.[214] They contend that measures of porn addiction merely measure how ashamed respondents are of their current sexual and masturbatory practices.[215] Some question if there is sufficient evidence to classify problematic or excessive internet use as an addiction,[216] while others argue that there is not enough high quality, conclusive evidence to indicate that pornography use can create the 'tolerance' and 'withdrawal' states in the brain that would constitute addiction. [217]

In 2020, Compulsive Sexual Behaviour Disorder (CSBD), was added to the World Health Organisation's (WHO) *International Classification of Diseases 11th revision* (ICD-11).[218] There is evidence to suggest that a large majority of people seeking treatment for CSBD have issues related to pornography use.[219] While some interpret the WHO's decision as a step towards the recognition of pornography addiction, others view this development as a clear indication that problematic pornography use should be understood as a compulsive behaviour disorder. The American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders has never recognised porn addiction (or, more broadly, sex addiction) as a phenomenon[220].

However, it is possible some young people may experience pornography as compulsive or as an addiction, or find those terms the best descriptors available, in that they feel the desire to engage with it is detracting from other areas of their life, and that their desire to view it causes overwhelming shame or discomfort. There is evidence of adults perceiving their online pornography use as problematic – reporting difficulty controlling their use and negative impacts in their lives due to use, such as mental health and wellbeing issues, problems in relationships and erectile issues.[221] Concerns about addiction were also raised by participants in our focus groups.

> 'Porn addictions are also bad, so in moderation it is okay if you can accept that you find it attractive or entertaining but don't expect the same with an actual partner' – eSafety focus group participant, 18

[214] McKee et al, *What do we know about the effects of pornography after fifty years of academic research?*, Routledge, 2022.
[215] McKee et al, *What do we know about the effects of pornography after fifty years of academic research?*, Routledge, 2022.
[216] van Rooij and Prause, 2014.
[217] De Alarcón et al., 2019; Van Rooij and Prause, 2014.
[218] Mead and Sharpe, 2020.
[219] Mead and Sharpe, 2020.
[220] American Psychiatric Association, *Diagnostic and statistical manual of mental disorders (DSM-5)*, American Psychiatric Publishing, Washington DC, 2013.
[221] S Hanseder and J Dantas, '*Males' lived experience with self-perceived pornography addiction: A qualitative study of problematic porn use*', International Journal of Environmental Research and Public Health, 2023, 20(2):1497, DOI: 10.3390/ijerph20021497.

‘Additionally, with how widespread online porn is, I think it contributes to people's porn addictions’ – eSafety focus group participant, 18

‘I think sometimes it can become an unhealthy habit where you get addicted in a sense’ – eSafety focus group participant, 16

Conclusion

Roadmap submissions and consultation sessions questioned existing assumptions about online pornography and children’s experiences of it, often suggesting a shift from binary characterisations (i.e., good/bad or unhealthy/healthy). The 16-18-year-old participants in eSafety’s survey and focus groups echoed the sentiment that binary approaches may overlook important nuances in children’s encounters and engagement with online pornography.[222]

Children, particularly older children, have complex relationships with online pornography. Understanding this relationship requires awareness of the broader context of children’s lives and online experiences. There are various individualised factors for children which may affect their experiences with online pornography and their risk, or actual experiences, of harm.

Current literature indicates that children commonly see online pornography before they are 18 and encountering it on a range of online services. While children may see or seek out online pornography for a variety of reasons, many see it unintentionally, resulting in negative feelings and experiences. This highlights the importance of respecting children’s agency to control their own online experiences, while also empowering and supporting them through education so they can understand and critically think about the content they see online.

The value of providing choice and control to children, parents and carers was a dominant theme in our consultations, as was supporting children to develop emotional and digital literacy skills to assess their experiences, reject harmful messages (e.g., gender violence and gender norms) and have greater control over their online experiences (e.g., using privacy and safety tools).

However, more research is needed. By developing a more complete understanding of children’s experiences, where unintentional encounters occur, and children may seek out online pornography, policymakers can design multi-faceted, targeted and effective measures that empower young people and minimise potential harms from online pornography. Further insights will support the development of measures that respect the evolving capacity of children, are informed by children’s lived experiences and respect their digital rights.

[222] Henry and Talbot, 2019.

Chapter 6: The digital ecosystem for accessing online pornography

Key Points

- There are multiple access points for online pornography within the digital ecosystem. The rate and risk of intentional or accidental encounters with online pornography varies across these access point. Similarly, the measures deployed across these access points to restrict children's access to online pornography and mitigate potential harmful effects also vary.
- Pornography websites rank in Australia's most visited websites. Most young people (70%) eSafety surveyed encountered online pornography on pornography sites.[223]
  - However, eSafety's research shows that many young people are also encountering sexually explicit content on social media platforms. For example, young people may receive friend requests and messages from accounts promoting pornography or use messaging apps to send each other links to pornography on other services.
  - Unintentional encounters also often occur through pop-ups on unrelated websites and by entering an incorrect web address on an internet search engine.
- Stakeholders raised several issues regarding access points to online pornography, including concerns with:
  - The effectiveness of age ratings, terms of service and efforts to prevent children from downloading age-inappropriate apps on app distribution services.
  - A change in user traffic patterns away from sites, which require some form of age assurance and towards those without access restrictions, search engine algorithms could end up listing non-compliant, harmful sites in their top search results.
  - Pornography still being accessible on services that do not allow it under their terms of service.

[223] eSafety, forthcoming.

- There is a need for a holistic approach which introduces measures up and down the digital stack, to capture the different pathways to accessing and encountering online pornography.
  - The reach of major pornography websites and the nature of the content freely available on their homepages, places significant responsibility on these companies to take reasonable steps to prevent children from accessing their services. Smaller pornography websites also have a responsibility to respect children's best interests and implement age-restricted access.
  - Search engines and messaging apps can play an important gatekeeper role in reducing children's access to this content, for example, through default safe search filters, warning messages and the blurring of explicit content.
  - Social media services have a responsibility to provide age-appropriate experiences for their users. This can be done using age assurance measures, nudging users regarding uploaded content which breaches the terms of service or community guidelines and by using effective content moderation tools.
  - Websites which may be accessed by children should give consideration to children accessing the site and should vet advertisements and pop ups to make sure children are not exposed to harmful content, including online pornography.

Overview

As explored in chapter 5, children encounter different types of online pornography in various environments and contexts.

In our consultations, stakeholders called for a multi-layered approach to restricting children's access to online pornography, which accounts for all the places, ways and reasons children might encounter this material, and opportunities for intervention across the entire digital ecosystem.[224]

Accordingly, this chapter explains the access points to online pornography. It outlines the complex and intersecting layers of the online industry, including the devices used to access the internet, the services that provide internet connectivity, and the platforms through which content is discovered, viewed, and shared. This chapter also highlights the extent to which various sections of the online industry are regulated under the *Online Safety Act 2021* (Cth) ('the Act').

[224] See Appendix 5.

The digital ecosystem

For any given image or video to appear online, a coordinated series of services across different companies are required, all of which have some ability to contribute to preventing or mitigating harm to children.[225] This includes the equipment or devices used to access the internet, the services which provide users access to the internet via an internet connection, and the platforms where content is discoverable.[226] For the purpose of readability, this section breaks down the various access points to online pornography as *enabling hardware and services* (e.g., devices, ISPs and hosting services) and *sites, apps and services* (e.g., search engines, social media services and websites).

Enabling hardware and services

Devices

In eSafety's 2018 research with Australian parents of children aged 2-17, 94% of those surveyed reported their child was using internet-enabled devices before the age of 4.[227] Devices may be shared among various users of different ages within a family, school or community, or used by one person exclusively.

According to Pornhub's 2022 insights report, mobile devices made up 97% of its global traffic for the year, with smartphones being 84% (of these, 52% were Android and 48% were Apple).[228] In Australia, 79% of Pornhub visits occurred on a smartphone, with 17% on a desktop computer and 4% on a tablet. Visits to Pornhub also occur via gaming consoles, with Sony PlayStation consoles making up nearly three quarters of these visits globally. As set out in chapter 7, eSafety anticipates increased uptake of virtual reality devices in the coming years which will provide more immersive online experiences, including for pornography.

Under the Act, devices are referred to as 'equipment'. Those who manufacture, supply, maintain or install equipment which Australians use to access services on the internet constitute one of the eight online industry sections which can be regulated under industry codes or standards.[229] See chapter 14 for further information about how the Act applies to devices, chapter 10 for information about other countries' mandates for device-level protections, and chapters 8, 11

[225] Canadian Centre for Child Protection, *Project Arachnid: Online Availability of Child Sexual Abuse Material*, 2021, p 9. https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/.
[226] 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. For a more comprehensive examination of the technology ecosystem, see Business for Social Responsibility and Global Network Initiative, *Human Rights Due Diligence Across the Technology Ecosystem*, 2022, available at: https://eco.globalnetworkinitiative.org/.
[227] eSafety Commissioner, *Supervising preschoolers online*, eSafety website n.d. https://www.esafety.gov.au/research/digital-parenting/supervising-preschoolers-online.
[228] Pornhub Insights, *The 2022 Year in Review*, 2022. https://www.pornhub.com/insights/2022-year-in-review.
[229] *Online Safety Act 2021* (Cth), s 135.

and 12 for a discussion about measures device providers can and do take to support children's safety.

Internet service providers (ISPS)

ISPs (including mobile phone network providers) are defined in the Act as providers which supply or propose to supply an internet carriage service to the public.[230] Commonly used ISPs include Aussie Broadband Group, Foxtel Management Pty Limited, Optus Group, Telstra Corporation, TPG Telecom Group and Vocus Group.[231] These services can be provided through fixed services (such as home, school, work or other public Wi-Fi) or mobile broadband (generally part of a mobile data plan).[232]

Modems (which connects a home network to the ISP) and routers (which enables devices to use that internet connection and talk to one another) also help devices connect to the internet. Many ISPs provide a combined modem/router that performs both functions in one device. Users can also purchase their own smart routers which include parental control settings to:

- limit the time children can access the internet
- block content using commercially available filters,
- manually configure block or allow lists.

The Australian Cyber Security Centre provides information on how users can set up their internet connection in a safe and secure manner.[233]

The Act includes different provisions which apply to ISPs, including industry codes or standards as discussed in chapter 14.

The Act also empowers eSafety to request or require ISPs to block access to material that promotes, incites, instructs in or depicts 'abhorrent violent conduct', such as murder or rape, if satisfied that the availability of the material is likely to cause significant harm to the Australian community.[234] As set out in chapter 10, regulators in other jurisdictions can require ISPs to block sites which have failed to comply with requirements to restrict children's access to online pornography.

[230] Online Safety Act 2021 (Cth), s 19.
[231] ACCC, *NBN Wholesale Market Indicators Report (March Quarter 2023)*, June 2023. https://www.accc.gov.au/by-industry/telecommunications-and-internet/national-broadband-network-nbn-access-regulation/nbn-wholesale-market-indicators-report/march-quarter-2023-report.
[232] For purposes of this report, we have focused on the 'last mile' ISPs which provide services directly to the public rather than the 'backbone' ISPs or transmission infrastructure companies which own and maintain the physical infrastructure.
[233] Australian Cyber Security Centre, *Protect yourself: Advice and information about how to protect yourself online*, ACSC website n.d. https://www.cyber.gov.au/protect-yourself.
[234] *Online Safety Act 2021* (Cth), Part 8.

Browsers

Browsers are software installed on devices to retrieve content from the internet and display it on a user's device. Sites, including internet search engine services, are accessed via a browser.

Currently, the most popular browsers in Australia are Google Chrome and Apple Safari, followed by Microsoft Edge, Samsung Internet and Mozilla Firefox.[235] Chrome and Safari are the most commonly used browsers to access Pornhub globally (with 48% and 42% of global traffic, respectively).[236]

Browsers play an important role in protecting user safety, privacy and security. Browsers are currently not one of the online industry sections regulated under industry codes or industry standards, although devices – which typically come with built-in browsers – are covered.[237]

Domain administrators and registrars

A domain name is what people type into a browser to find a site (for example, www.esafety.gov.au). When a person or company first establishes a website, they must purchase and register a domain name through a domain name registrar. Details about the site and its registrar are included in a domain name registry or database. Registry administrators develop and apply the rules for domain names in their scope. For example, auDA administers domain names ending in the '.au' country code.[238]

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for coordinating the names and numbers that relate to internet domains, including the approximately 1,500 generic top-level domains such as .com, .net and .org.[239] Verisign, which is headquartered in the United States but has an Australian office, is the administrator for the '.com' top-level domain and accordingly for the top three most accessed pornography sites in Australia (as at November 2022): Pornhub.com, Xvideos.com, and Xxnx.com. Their respective registrars are EuroDNS (based in Europe), and Moniker and GoDaddy (based in the United States).

Domain administrators and registrars are not currently captured within the Act. However, the role they have adopted in addressing Domain Name System (DNS) abuse could be extended to helping to safeguard children, as discussed in chapter 12.

[235] Similarweb, *Top Websites Ranking: Most Visited Websites In The World,* 2022, available at: https://www.similarweb.com/top-websites/

[236] Pornhub Insights, *The 2022 Year in Review*, 2022.

[237] ACCC, *Digital platform services Inquiry – Interim report No. 3: Search defaults and choice screens*, 2021,. https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-Inquiry-2020-2025/digital-platform-services-Inquiry-september-2021-interim-report.

[238] See; auDA, *Home,* available at: https://www.auda.org.au/.

[239] ICANN, *What ICANN Does and Doesn't Do*, 2012. https://www.icann.org/en/system/files/files/what-icann-does-22jun12-en.pdf.

Hosting services

Hosting services provide data storage and other computing support to enable sites to exist on the internet. The services hosting the top three pornography sites visited from Australia are Reflected Networks (based in the United States), ServerStack (headquartered in the United States, but hosting Xvideos in the Netherlands) and NKL Associates S.R.R. (based in Czech Republic).

Under the Act, the provider of a hosting service is defined as a person who hosts stored material that has been provided on a social media service, relevant electronic service or designated internet service (which includes messaging services, gaming services and other sites and apps).[240] There are several provisions in the Act which apply to hosting services regardless of their location, including the power to give them a removal notice requiring them to cease hosting class 1 material. However, industry codes or standards developed under the Act only apply to services which host material in Australia.[241] Due to Australia's online regulatory environment, it is uncommon for pornography to be hosted in Australia. Measures hosting services could undertake to restrict children's access to online pornography are suggested in chapter 11 and 12.

App distribution services

An app distribution service enables people to download applications onto their devices.[242] The Act defines an app distribution service as a service that enables end-users to download apps, where the download of the apps is by means of a carriage service.[243] Apps may be free or paid, and cut across a wide range of categories, including social media, gaming, messaging, and dating.

The most popular app distribution services are the Apple App Store and Google Play. These services review apps and apply age-based content ratings.[244] Apps must meet the App Store Review Guidelines prior to becoming publicly available.[245] Neither the App Store nor Google Play's terms of service permit apps whose main purpose is to provide pornography, though both allow some apps whose terms of service permit sexually explicit material, including pornography.[246]

[240] Online Safety Act 2021 (Cth), s 17.
[241] Online Safety Act 2021 (Cth), s 134(f).
[242] Online Safety Act 2021 (Cth), s 5.
[243] Online Safety Act 2021 (Cth), s 5.
[244] Apple, *Get started: Age ratings*, Apple App Store. https://apps.apple.com/is/story/id1440847896; Google, *Apps & Games content ratings on Google Play*, Google Play Help. https://support.google.com/googleplay/answer/6209544.
[245] Apple, *App Store review guidelines*, Apple App Store. https://developer.apple.com/app-store/review/guidelines; Google, *Providing a safe and trusted experience for everyone*, Google Play Help. https://play.google.com/about/developer-content-policy/.
[246] Apple, *App Store Review Guidelines*, 1.1.4, 1.2; Google, *Inappropriate content*, Play Console Help. https://support.google.com/googleplay/android-developer/answer/9878810?sjid=6597965075595576571-AP.

Some of most downloaded apps that are used by children are explored later in this chapter. Often, the default minimum age set by the app differs from the age rating assigned by the app distribution service. For example, Discord, Reddit and Twitter permit users aged 13+ to create accounts, but these apps are rated 17+ on the Apple App Store due to the nature of the content they allow. App store age ratings are a guide only, and users are not prevented from downloading specific apps if they are below the rated age for the app.

The stakeholders we consulted raised several issues in relation to app distribution services. Some questioned the effectiveness of age ratings and efforts to prevent children from downloading age-inappropriate apps. There were also perceptions of inconsistency and a lack of transparency in applying policies – including claims of unfair or potentially anti-competitive practices in relation to third-party safety apps.

Several provisions under the Act apply to app distribution services, including the development of applicable industry codes or standards.[247] The eSafety Commissioner can also give an app removal notice to an app distribution service if satisfied there were two or more times during the previous 12 months when end-users in Australia could use the service to download an app that facilitates the posting of 'class 1 material' and the relevant app failed to comply with one or more removal notices during that period.[248]

The measures app distribution services are currently applying, or could undertake, to restrict children's access to online pornography are discussed in chapters 8, 11 and 12.

Where online pornography can be found and shared

There are many different sites, apps, or services where online pornography can be found and shared. The Act breaks these down into three categories:

- **social media services**, defined as services which allow end-users to post material and to interact with other end-users, where the primary purpose of the service is enabling online social interaction between two or more end-users.[249]
- **relevant electronic services**, defined as services that enable end-users to play online games or with each other or communicate with each other by email, instant message, SMS, MMS or chat.[250]
- **designated internet services**, which covers other services that allow end-users to access material on the internet.[251]

[247] Online Safety Act 2021 (Cth), s 202, s 135(2)(e).
[248] Online Safety Act 2021 (Cth), s 128.
[249] Online Safety Act 2021 (Cth), s 13.
[250] Online Safety Act 2021 (Cth), s 13A.
[251] Online Safety Act 2021 (Cth), s 14.

Measures specific to these service categories are being established through the development of industry codes or standards. Phase 2 of codes and standards development (due to commence in late 2023) will be more relevant to the objectives of the roadmap. More detail on the codes and standards is available in chapter 14.

The evidence-base canvassed in this report demonstrates children are encountering pornography in all of these online environments – including on services which disallow it. However, the types of interventions which may be most effective and proportionate may differ depending on the context.

Therefore, for the purposes of this report, we will consider the following categories of services:

- services where the primary purpose is providing pornography
- services where the primary purpose is not providing pornography, but pornography is permitted content
- services where pornography is not permitted content.

There are complicated interrelationships between various services. A user's journey to accessing or encountering online pornography may involve several intersecting services whose terms of service may vary.

Because popular mainstream services offer easy access to a large potential audience, they are often used to attract followers and subsequently redirect them to services which permit online pornography or other types of content. For example, many creators of pornography on OnlyFans first attract followers through Instagram or Snapchat, which do not permit such content.[252]

While the local adult industry has emphasised their efforts to avoid engaging with underage users on social media,[253] 16-18-year-olds in our focus groups said it is common to receive friend requests and messages from accounts promoting pornography. Children also use messaging apps to send each other links to pornography on other services. One in three (34%) of our survey respondents first encountered online pornography when it was shared with them by their peers and/or in social networks.

Stakeholders emphasised this is why a whole-of-ecosystem approach which considers different pathways to pornography is important.

[252] FriendsOnly, *How can you promote your onlyfans on Instagram?*, Medium, 2022. https://medium.com/how-to-make-money-with-videoblog/how-can-you-promote-your-onlyfans-on-instagram-680e06f78549.

[253] Scarlet Alliance, *Submission on the draft RAS Declaration and explanatory statement*, 2021. https://www.esafety.gov.au/sites/default/files/2021-09/Scarlet Alliance RAS submission %28September 2021%29_0.pdf

Internet search engine services

The vast majority (93%) of visits to websites start within a search engine,[254] a software system that enables people to search for words or phrases to help them find the information they are looking for online.

The most popular search engine globally, and within Australia, is Google which accounts for 93% of Australian online searches.[255] Other search engines include Bing and DuckDuckGo.

Children may use search engines to seek out pornography, or they may encounter it unexpectedly when searching for something else. Of the 16-18-year-olds we surveyed who had seen online pornography, 59% said they had intentionally searched for it.

While privacy legislation prevents companies from tracking children online, according to general online search data from users of all ages in Australia, there are 1,200,000 average monthly searches for 'porn', in addition to the following searches for specific pornography sites discussed later in this chapter:

- 13,600,000 average monthly searches for 'pornhub'
- 1,830,000 average monthly searches for 'xvideos'
- 1,500,000 average monthly searches for 'xhamster'
- 1,220,000 average monthly searches for 'chaturbate'. [256]

Some focus group participants suggested that seeing online pornography for the first time may generate a curiosity to search for more.

> 'Young people before exposure don't really search for it, but once introduced, people are curious' – eSafety focus group participant, 16
>
> 'A lot of people show their friends this kind of stuff, even if it's as a joke at first, but quite often people get curious and start searching themselves' – eSafety focus group participant, 16

The content that emerges in search results varies depending on many factors and signals, including the specific search terms entered and the popularity of matching pages.

In eSafety's consultations, multiple stakeholders expressed the concern that users whose search for pornography initially leads them to sites with age assurance requirements may seek

[254] V La Barbera, *8 SEO stats that are hard to ignore*, imFORZA,. https://www.imforza.com/blog/8-seo-stats-that-are-hard-to-ignore/.
[255] Similarweb, *Search engines market share in Australia*, 2023. https://www.similarweb.com/engines/australia/.
[256] Semrush, *Semrush: Online marketing can be easy.* https://www.semrush.com/.

to avoid these measures and continue searching until they find sites without such measures. Stakeholders pointed out this may cause those non-compliant sites to be prioritised over compliant sites in search results, driving more users to sites which lack safety measures and may also host more extreme or violent forms of pornography.

Accordingly, it is important for search engines to be engaged in efforts to promote regulatory compliance among other sections of the online industry to avoid unintended consequences. The measures search engines are (and could be) applying to restrict children's access to online pornography are discussed in chapters 8, 11 and 12.

Under the Act, the eSafety Commissioner can issue a link deletion notice to a search engine if satisfied there were two or more times during the previous 12 months when end-users in Australia could access 'class 1 material' using a link provided by the service and the relevant site failed to comply with one or more removal notices during that period.[257] As explained in chapter 14, 'class 1 material' can include pornography that is demeaning, violent or which depicts certain fetishes. However, the eSafety Commissioner prioritises the investigation and removal of seriously harmful content such as child sexual exploitation material.[258]

Services whose primary purpose is providing online pornography

The nature of online pornography and the contexts within which it is produced, shared, sold and consumed vary greatly. eSafety consulted with large international online pornography services, as well as local industry bodies representing Australian sex workers, pornography producers and performers. These consultations highlighted differing perspectives between the domestic and international industries.

Eros Association, an association for the adult industry in Australia, submitted that many local producers of content are female and operate as sole trader producer-performers.[259] In comparison, the international landscape is dominated by pornography 'tube sites'. For example, Mindgeek, a Canadian company, employs over 1,800 people worldwide. It owns Pornhub, a globally popular aggregator sites for online pornography, several other aggregator sites, and multiple major production companies such as Brazzers and Reality Kings. According to Mindgeek, its websites receive over 115 million daily visitors and serve over 3 billion advertising impressions.[260]

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

[257] Online Safety Act 2021 (Cth), s 124.
[258] eSafety Commissioner, *Online Content Scheme: Regulatory Guidance*, 2021. https://www.esafety.gov.au/sites/default/files/2021-12/eSafety-Online-Content-Scheme.pdf.
[259] Eros Association, *Submission on the draft RAS Declaration and explanatory statement*, 2021. https://www.esafety.gov.au/sites/default/files/2021-09/Eros Association RAS submission %28September 2021%29_0.pdf
[260] MindGeek, *A leader in Web design, IT, Web development and SEO*, 2023. https://www.mindgeek.com/.

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.

To ascertain which pornography-specific services children in Australia may pose the greatest risk in terms of accessing online pornography, eSafety identified the top five most visited pornography sites in Australia as of November 2022, according to Similarweb.[261]

Pornhub

Pornhub is owned by Mindgeek S.A.R.L and part of the larger Mindgeek organisation, headquartered in Luxembourg with offices in Nicosia, London, Montreal, Bucharest and Los Angeles. Pornhub has also submitted a notification to Cyprus indicating it is based there for purposes of the European Audiovisual Media Services Directive (AVMSD), discussed in chapter 10.

According to the site, Pornhub is 'the most complete and revolutionary porn tube site'. It features a mix of professional and amateur content which can be viewed for free and without signing up – including on its home page. Users can also create an account and subscribe to a premium service for a fee.

As at November 2022, Pornhub was the most popular pornography site in Australia and the 14th most visited website from Australia overall.[262] Pornhub is also one of the most popular sites worldwide, with an estimated 33 million EU monthly users[263] and 2.2 billion monthly total visits worldwide.[264]

In the 2021-22 financial year, eSafety received 63 reports from members of the public about sexually explicit, extreme, offensive or adult content on Pornhub.[265] France and Germany have taken regulatory action against Pornhub for allegedly failing to restrict children's access. Pornhub also has the potential to be considered under the UK's Audiovisual Media Services Regulations in the future as discussed in chapter 10.

eSafety consulted with representatives from Mindgeek for this report.

Xvideos.com

[261] Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.
[262] Similarweb, *Top websites ranking: most visited websites in Australia,* November 2022.
[263] Pornhub, *EU Digital Services Act*, 2023. https://www.pornhub.com/information/eu_dsa.
[264] Similarweb, *Top websites ranking: most visited websites in the world*.
[265] Consistent with our regulatory guidance, and as explained in chapter 14, eSafety generally exercises discretion not to investigate reports of individual items of pornographic content hosted outside of Australia, to focus our resources on investigations into child sexual exploitation and pro-terror material.

Xvideos is owned by WGCZ Holdings, based in the Czech Republic. It features both professional and amateur content which can be viewed for free and without signing up – including on its home page. Users can also create an account and subscribe to a premium service for a fee.

As of November 2022, Xvideos was the second most popular pornography site in Australia and the 20th most visited website from Australia overall.[266] It was also the top-ranked pornography site in the world.[267]

In the 2021-22 financial year, eSafety received 36 reports from members of the public about sexually explicit, extreme, offensive or adult content on Xvideos. France has taken regulatory action against Xvideos for failing to restrict children's access, as discussed in chapter 10.

Xnxx.com

Xnxx is also owned by WGCZ Holdings. It features both professional and amateur content which can be viewed for free and without signing up – including on its home page. Users can also access paid content with a credit card.

As of November 2022, Xnxx was the third most popular pornography site in Australia (and worldwide) and the 21st most visited website from Australia overall.[268]

In the 2021-22 financial year, eSafety received 14 reports from members of the public about sexually explicit, extreme, offensive or adult content on Xnxx. France has taken regulatory action against Xnxx for failing to restrict children's access, as discussed in chapter 10.

xHamster.com

xHamster is owned by Hammy Media, based in Cyprus. This site features both professional and amateur content. All content is free. There is the option to create an account.

As of November 2022, xHamster was the fourth most popular pornography site in Australia (and worldwide) and the 43rd most visited website from Australia overall.[269]

In the 2021-22 financial year, eSafety received 13 reports from members of the public about sexually explicit, extreme, offensive or adult content on xHamster. France and Germany have taken regulatory action against xHamster for failing to restrict children's access, as discussed in chapter 10.

eSafety consulted with representatives from Hammy Media for this report.

[266] Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.
[267] Similarweb, *Top websites ranking: most visited websites in the world*, November 2022.
[268] Similarweb, *Top websites ranking: most visited websites in the world,* November 2022; Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.
[269] Similarweb, *Top websites ranking: most visited websites in the world,* November 2022; Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.

Chaturbate.com

Chaturbate is owned by Triplebyte and is based in the US. Chaturbate (a portmanteau of chat and masturbate) provides live webcam performances, typically featuring nudity and/or sexual activity. Some live streams are free for users, while others require payment. Users can send tokens or money to performers.

As of November 2022, Chaturbate was the fifth most popular pornography site in Australia, but it did not feature within the top 50 most visited websites overall.[270] Similarweb's February 2023 data indicated Chaturbate had fallen in the rankings, replaced by realsrv.com as the fifth most popular pornography site in Australia.[271]

Given the reach of these five businesses – and the nature of the content freely available on their homepages they have a significant responsibility to take reasonable steps to prevent children from accessing their services. The types of age assurance and complementary safety tools they could employ for these purposes, and examples of some of the actions services are already taking, are set out in chapters 8, 11 and 12. As our stakeholders emphasised in consultations, and as explored further in chapter 14, a one-size approach for all businesses is unlikely to work.

Other online services which allow pornography or sexually explicit content

In addition to services which have a primary purpose of hosting and sharing pornography, there are many other broader-purpose services which permit some forms of sexually explicit content, including pornography. As discussed throughout the report, this is not inherently harmful. Social media and other online services offer important spaces for people to discuss, learn about, experience and explore their sexuality[272]. However, these spaces should be carefully designed and moderated to ensure they provide safe, age-appropriate and consensual experiences.

The following broader-purpose services which allow pornography participated in eSafety's consultations. The measures these companies take to protect children from harmful content are detailed in chapters 8 and 11.

Discord

Discord is a social chat platform commonly used by online gamers, which lets users create a profile and interact with other users via online messaging, voice or video chat. Users can share

[270] Similarweb, *Top websites ranking: most visited websites in the world,* November 2022; Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.
[271] Similarweb, *Top websites ranking: most visited websites in Australia*, November 2022.
[272] See Appendix 5; eSafety, forthcoming research.

images, files and links to other services. Discord hosts servers on a wide variety of interests, with a reported 190 million monthly active users globally.[273]

Discord allows users aged 13 and above. Under Discord's terms of service 'all adult content posted to Discord [is required to] be kept behind an age-restricted gate'.[274]

OnlyFans

OnlyFans is a content subscription service, advertised as a way for content creators of any genre to monetise their content and receive support or money direct from viewers and fans. Some content creators are sex workers and/or performer-producers of pornography.[275] OnlyFans has a minimum user age of 18.

Users who access the service, or 'fans', can subscribe to see exclusive content from creators for a monthly subscription fee. As of December 2020, OnlyFans reported it had 85 million registered users worldwide.[276]

While it was reported that OnlyFans briefly considered changing its policies to ban sexually explicit content in 2021, this decision was reversed and it currently permits pornography.[277]

Reddit

Reddit is described as a social news aggregation, content rating and discussion website. It is broken up into more than a million communities known as 'subreddits,' where people can share news and content or comment on other people's posts.[278] It has 52 million daily active users and about 430 million users who use it once a month.[279]

According to research released by the UK Children's Commissioner in January 2023, of the 16-21-year-olds who had seen pornography, 17% reported they had seen it on Reddit.[280] Reddit was also mentioned by our focus group participants as a platform where pornography can be accessed.

[273] Stefan Campbell, *How many people use Discord?*, The Small Business, 2023. https://thesmallbusinessblog.net/discord-statistics/.

[274] Discord, *Accessing an Age Restricted Server FAQ*, Discord Support, 2022. https://support.discord.com/hc/en-us/articles/1500005292701-Accessing-an-Age-Restricted-Server-FAQ.

[275] M Boseley, *'Everyone and their mum is on it: OnlyFans booms in popularity during the pandemic'*, The Guardian, 23 December 2020. https://www.theguardian.com/technology/2020/dec/23/everyone-and-their-mum-is-on-it-onlyfans-boomed-in-popularity-during-the-pandemic; CNN, *'Sex workers helped popularize OnlyFans. Now their future on the platform is uncertain'*, 9news.com.au, 2021. https://www.9news.com.au/technology/onlyfans-bans-sexually-explicit-content-sex-workers-losing-income/af764bc9-b026-4770-b778-31ebf13141a5.

[276] Boseley, '*Everyone and their mum is on it: OnlyFans booms in popularity during the pandemic*', 2020.

[277] E Barry, '*Why OnlyFans Suddenly Reversed its Decision to Ban Sexual Content*', *Time*, 26 August 2021. https://time.com/6092947/onlyfans-sexual-content-ban/.

[278] J Widman, *What is Reddit?*, Digitaltrends, 2022. https://www.digitaltrends.com/computing/what-is-reddit/.

[279] D Curry, *Reddit Revenue and Usage Statistics (2023)*, Business of Apps, 2023. https://www.businessofapps.com/data/reddit-statistics/.

[280] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.

Reddit allows users aged 13 and up. Reddit permits pornography but requires it to be tagged as ‘not safe for work’ (‘NSFW’) so it can be filtered out for younger users and those who do not wish to see it.[281]

Twitter

Twitter is a social media service which allows users to share posts and follow other users. Posts can include extra content such as images, video, links, keywords, location information and polls. As of April 2022, there were a reported 5.8 million active monthly Twitter users in Australia.[282]

Twitter allows some adult content (including pornography) to be posted on the site, if it is appropriately tagged. According to the UK Children’s Commissioner’s research, Twitter is the most common online service for 16-21-year-olds to encounter online pornography. Of those who had seen pornography, 41% reported having seen it on Twitter.[283] The report also refers to internal Twitter documents which suggest that 13% of the content on Twitter constitutes pornography.

Online services which do not allow pornography.

Finally, there are services whose terms of service, or rules, prohibit posting or sharing pornography. Despite having these policies in place, many stakeholders raised during consultation that children can easily access or share online pornography through these services. eSafety’s direct research with 16–18-year-olds found it is common for children to have seen pornography on social media sites, or be sent online pornography through social media sites.

The following services which do not allow pornography participated in eSafety’s consultations for this report. Any measures taken by these companies to protect children from harmful content are detailed in chapters 8 and 11.

Facebook

Facebook is a social media service that lets users create a page about themselves, an organisation or group. Users can add friends, write on people’s pages, share photos and videos including live videos and send private messages (through Meta’s ‘Messenger’ service’). Facebook and Messenger are owned by parent company Meta and based in the United States. Facebook has approximately 2.96 billion monthly active users.[284]

[281] Reddit, *Reddit Content Policy* n.d. https://www.redditinc.com/policies/content-policy.
[282] K Tong, *How relevant is Twitter to most people?*, ABC, 2022. https://www.abc.net.au/news/2022-04-27/how-relevant-is-twitter-to-most-people/101018420.
[283] UK Children’s Commissioner, *‘A lot of it is actually just abuse’: Young people and pornography*, 2023.
[284] Meta, *Adult nudity and sexual activity: How prevalent were adult nudity and sexual activity violations?,* Meta Transparency Centre, 2022. https://transparency.fb.com/data/community-standards-enforcement/adult-nudity-and-sexual-activity/facebook/#prevalence.

The minimum age to use Facebook is 13. Facebook does not allow the display of nudity and sexual content, either explicit or implied. Nudity in a health context or in digital art is allowed but restricted to over 18s and preceded with a warning. According to its Q4 2022 transparency report, Facebook acted on 29.2 million pieces of adult nudity and sexual activity content between October and December 2022. Of this, 94.1% was proactively detected by Facebook and 5.9% was reported by users.[285]

Instagram

Instagram is a social media service designed for people to share photos and videos. Users can upload and share photos, images or videos in several formats and send private messages. Instagram 'Stories' allows users to post photos and videos that disappear after 24 hours. It is owned by parent company Meta and based in the United States.

The minimum age to use Instagram is 13. Instagram does not allow depictions of sexual intercourse. Some nudity is allowed in particular contexts.[286] According to its Q4 2022 transparency report,[287] Instagram acted on 10.8 million pieces of adult nudity and sexual activity content between October and December 2022. Of this, 95.5% was proactively detected by Instagram and 4.5% was reported by users.

A 2023 report by the UK Children's Commissioner found that 33% of survey participants (aged 16-to-21-years-old) who had previously seen pornography had seen it on Instagram, making it the third most common place to see pornography, behind Twitter (41%) and dedicated pornography sites (37%).[288] eSafety's 16-18-year-old focus groups participants also shared they had seen online pornography on Instagram and other social media services.

Roblox

Roblox is a global game-creation platform that allows users to design their own games and play a wide variety of games created by other users. The platform hosts millions of user-created games and virtual worlds covering a wide variety of genres, from traditional racing and role-playing games to simulations and obstacle courses. Roblox also allows players to buy, sell and create virtual items. Roblox estimates it has 67.3 million active daily users worldwide.[289]

Roblox does not have a minimum age, but its terms of service provide that anyone under 18 may only use the service with the consent of a parent or guardian.[290] The platform is popular

[285] Meta, *Adult nudity and sexual activity: How prevalent were adult nudity and sexual activity violations?.*
[286] Instagram, *Community Guidelines*. https://help.instagram.com/477434105621119/.
[287] Meta, *Adult nudity and sexual activity: How prevalent were adult nudity and sexual activity violations?*
[288] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.
[289] Roblox, *Roblox Reports February 2023 Key Metrics*, 2023. https://ir.roblox.com/news/news-details/2023/Roblox-Reports-February-2023-Key-Metrics/default.aspx.
[290] Roblox, *Roblox Terms of Use*, n.d. https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use.

with children, with 54.25% of Roblox users being under the age of 13.[291] There have been several media reports in recent years regarding alleged instances of sexual content, conduct. and grooming on Roblox.[292]

Snapchat

Snapchat is a social media service that lets users send images, videos or instant text messages to friends. These images, videos and messages are only available for a short period of time once they are opened. Snapchat reports 750 million active monthly users globally.[293]

Snapchat is an 18+ service, though children over 13 can use the platform with parental consent. Nudity and sexual content are not allowed under the community guidelines however such content can still be accessed on the app through peer-to-peer sharing (both links and personal images).[294]

In its most recent transparency report, Snapchat said it received 7.53 million reports of content that violated its sexually explicit content guidelines, making this Snapchat's top reason for content removals. Of this, 4.3 million pieces of content were removed, and 2.37 million accounts were banned. Snapchat estimates that 3 in every 10,000 pieces of content shared on Snapchat violate its guidelines.[295]

A 2023 report by the UK Children's Commissioner found that 32% of survey participants (aged 16-to-21-years-old) who had previously seen pornography had seen it on Snapchat.[296] This was also raised in eSafety's focus groups, including by one 16-year-old participant who was also aware of accounts which contacted teenage users and encouraged them to access pornography, including some paid content.

TikTok

TikTok is a social media app for creating and sharing short videos. Users can create and share videos between 3 seconds and 10 minutes long, live stream (for over 18s) and message users

[291] D Ruby, *Roblox Statistics 2023 – (Users, Revenue & Trends)*, Demand Sage, 2023, https://www.demandsage.com/how-many-people-play-roblox/.

[292] J Clayton and J Dyer, *'Roblox: the children's game with a sex problem'*, BBC, 15 February 2022, https://www.bbc.com/news/technology-60314572; J Jargon, *'Roblox Struggles With Sexual Content. It Hopes a Ratings System Will Address the Problem'*, Wall Street Journal, 17 April 2021. https://www.wsj.com/articles/roblox-struggles-with-sexual-content-it-hopes-a-ratings-system-will-address-the-problem-11618660801; C Fitzsimmons, *'Sometimes I experience nothing, other times it's rampant': sexual material warning on Roblox'*, Sydney Morning Herald, 23 January 2021. https://www.smh.com.au/technology/sometimes-i-experience-nothing-other-times-it-s-rampant-sexual-material-warning-on-roblox-20210123-p56wcq.html.

[293] S Perez, *Snapchat announces 750M monthly active users*, TechCrunch, 2023. https://techcrunch.com/2023/02/16/snapchat-announces-750-million-monthly-active-users/.

[294] Snap Inc., *Community Guidelines & Rules*, January 2023. *https://values.snap.com/privacy/transparency/community-guidelines*.

[295] Snap Inc., *Snapchat Transparency Report: July 1 - 31 December 2022*, June 2023. https://values.snap.com/privacy/transparency.

[296] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.

they follow and who follow them back. TikTok is owned by ByteDance, headquartered in China. TikTok has more than 1 billion monthly active users.[297]

TikTok's minimum age is 13 years old. Nudity, pornography, and sexually explicit content is prohibited, as well as content depicting or supporting non-consensual sexual acts, the sharing of non-consensual intimate imagery, and adult sexual solicitation.

Between October and December 2022, TikTok removed 85.7 million videos for violation of its community guidelines. Of these, 12.8% of these videos were removed under its Adult Nudity and Sexual Activities policy, with 92.6% proactively detected by TikTok and 78.8% removed before the content had been viewed.[298]

A 2023 report by the UK Children's Commissioner found that 23% of survey participants (aged 16-to-21-years-old) who had previously seen pornography had seen it on TikTok.[299] Encountering pornography on TikTok was also raised in eSafety's focus groups.

YouTube

YouTube is a user-generated video sharing platform that allows people to discover, watch and share videos. Users can create their own channel and subscribe to the channels of other people or organisations. YouTube is owned by Google and is headquartered in the United States.

The minimum age to use YouTube is 13. However, users of any age can create a YouTube account with parental consent and anyone can access YouTube without signing in.

According to YouTube's most recent transparency report, it terminated 5.8 million channels and removed 207.8 million pieces of content between July and September 2022, for violating its Community Guidelines. Approximately 3% of terminated channels and 13.7% of removed content were due to nudity and/or sexual content.[300]

Conclusion

This chapter demonstrates that there are a wide range of access points for online pornography.

There are complex and intersecting responsibilities for protecting children, with devices, app stores, browsers, pornography websites, and social media services (among others) forming layered access points to this content. A holistic approach, which introduces measures up and

[297] Chloe West, *27 TikTok stats marketers need to know in 2023*, Sprout Social, 2023. https://sproutsocial.com/insights/tiktok-stats/.

[298] TikTok, *Community Guidelines Enforcement Report*, 2022. https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2022-4/.

[299] UK Children's Commissioner, *'A lot of it is actually just abuse': Young people and pornography*, 2023.

[300] Google, *YouTube Community Guidelines enforcement*, 2023. https://transparencyreport.google.com/youtube-policy/removals?hl=en.

down the digital stack, is needed to address the different pathways for children to access and encounter online pornography.

As discussed in forthcoming chapters, there are many proactive technical measures that could be deployed across the digital ecosystem to mitigate children's access to online pornography.

Chapter 7: The future of online pornography

Key Points

- Developments in generative artificial intelligence, internet decentralisation, immersive technologies and other technology trends have the potential to change how online pornography is accessed and consumed. These developments could create new and enhanced risks to children, as well as generating new opportunities for keeping them safe.
- It is unclear what a future 'metaverse' may look like, but it has the potential to blur the lines between sexual content and sexual experiences. It could make online pornography feel substantially more visceral, intense and realistic, and heighten its impacts on children who encounter it.
- It is important that measures to prevent and mitigate harms to children associated with online pornography are designed to incorporate emerging technologies.

Overview

Consistent with the guiding principles of this report, this chapter explores some of the current and emerging developments which may create new challenges and new opportunities for preventing and mitigating harm to children from online pornography. It examines how these developments could change the nature of online pornography and the way people interact with it.

The chapter focuses on immersive technologies and the metaverse, given their potential to create high-impact, hyper-realistic online experiences that blur the lines between content and activity, and what is real and what is virtual. It considers current immersive devices, environments and safety tools, and explores how future iterations may be shaped by existing high-impact games that blend sexual content, conduct and violence, particularly against women and sex workers. It also contemplates the impact of decentralised (web3) technologies, the use of self-sovereign identity for age verification, and artificial intelligence (AI) particularly generative AI and deepfake technologies.

These technologies will not operate in isolation. As they converge, they may mutually reinforce risks to children. For example, companies building metaverse platforms will rely on AI to create realistic immersive environments and non-player characters (NPCs) with digital identities at scale. Creators may use AI to create intimate images, sounds, or sexually explicit content, conduct or contact depicting real or computer-generated people and identities in synthetic pornography.[301] User engagement with this content and the expanding Internet of Things will produce a trove of personal data, which may be fed to algorithms to serve those users with recommendations for similar or targeted content.[302]

These technologies – both individually and in combination – carry safety, privacy and security risks and regulatory challenges. Depending on their design, they could increase the risk of children encountering pornography and experiencing intensified forms of harm as a result. In addition, children could use tools such as AI to generate pornographic images. Although outside of the scope of this report, there are also heightened risks of child sexual exploitation, abuse, and grooming. However, these technologies can also be used to mitigate the risk of children encountering pornography and other serious forms of online harm such as child sexual exploitation.

Principles like proportionality, respect for human rights, and data minimisation will continue to be critical in the design and deployment of such technologies. Ongoing work with both start-ups and mature companies is essential for increasing Safety by Design uptake, proactive identification of emerging threats, and investment in ongoing improvement. Technological, regulatory and educational interventions will need to adapt to the changing online environment. Regulatory frameworks and measures also need to be future-proofed to account for technical and social developments.

eSafety's Future Focus

eSafety consults with experts and analyses new research and policy developments to ensure its content and programs respond to current online safety challenges.

In line with the Commissioner's functions under section 27 of the Act, eSafety publishes its approach to selected tech trends and challenges and offers guidance for industry and the public in position statements hosted on our website.

eSafety's Safety by Design initiative is fundamental to helping services to proactively identify and mitigate risks from emerging technologies. Safety by Design is built to be technology-agnostic, so its principles can be applied across the existing online ecosystem and its future iterations.

[301] H Farid, *Text-to-image AI: Powerful, easy-to-use technology for making art – and fakes*, The Conversation, 2022. https://theconversation.com/text-to-image-ai-powerful-easy-to-use-technology-for-making-art-and-fakes-195517.

[302] M Zawish, FA Dharejo, SA Khowaja, K Dev, S Davy, NMF Qureshi and P Bellavista, *'AI and 6G into the Metaverse: Fundamentals, challenges and future research trends',* arXiv preprint, 2022, arXiv:2208.10921.

Generative AI and customisable pornography

Consistent with the Inquiry, the primary focus of this report is children's access to online pornography created by adults, often for commercial purposes, and generally featuring real performers. As set out in chapter 2, sexually explicit images that children take of themselves or of other children are out of scope. We note that children themselves often do not differentiate between content and activity involving those under the age of 18 (which would be classified as child sexual exploitation), versus content and activity involving adults.

Recent developments in generative AI technologies – which enable the rapid generation of written content, images, video and audio based on natural language voice or text commands – add another layer of complexity to this discussion. Through these technologies, users – including children – can now access or generate digital pornography to their specifications. With this comes the risk of manufacturing virtual partners, activity, or content which reflect harmful views, biases and behaviours.[303] In particular, open-source generative AI models released with public code pose certain risks, as they allow anyone to adapt this technology and remove guardrails.

Some scholars state that AI is already capable of generating synthetic images of faces that are indistinguishable from real faces.[304] For example, deepfake technologies draw on multiple photos or recordings of a person to model and create realistic content.[305] Generative AI and deepfakes have already been used to create pornography, including of real people - particularly of women in the public spotlight and typically without their consent.[306] While these applications can enhance creative expression, without proper consideration of their safety implications and subsequent introduction of risk mitigations, they can be misused to cause serious harm.

Deepfakes and pornography

While deepfakes can be weaponised for various reasons, research conducted in 2019 showed that 96% of deepfakes were pornographic.[307]

[303] B Wassom, *Augmented reality law, privacy, and ethics: Law, society, and emerging AR technologies*, Syngress, 2014, Part C: AR & Society.
[304] S Nightingale and H Farid, *'AI-synthesized faces are indistinguishable from real faces and more trustworthy'*, Proceedings of the National Academy of Sciences, 2022, 119(8):e2120481119, DOI: 10.1073/pnas.212048111.
[305] eSafety Commissioner, *Deepfakes – position statement*, January 2022. https://www.esafety.gov.au/industry/tech-trends-and-challenges/deepfakes.
[306] H Farid, *'Creating, Using, Misusing, and Detecting Deep Fakes'*, Journal of Online Trust and Safety, 2022, 1(4), DOI: 10.54501/jots.v1i4.56.
[307] H Ajder, Giorgio Patrini, F Cavalli and L Cullen, '*The State of Deepfakes: Landscape, Threats, and Impact*', Deeptrace, 2019. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

One prominent case entailed a popular Twitch streamer being caught accessing deepfakes of several female streamers. He later admitted to buying pornographic deepfake videos of two 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.[308]

It is critical that protections keep pace with advances in deepfake and generative AI technology.

Virtual reality (VR) applications also exist which enable users to craft sexualised environments and characters. In some instances, applications have reportedly allowed users to simulate the sexual abuse of children.[309] By enabling more realistic and customisable VR experiences, generative AI is increasing risks of harm to children. It is possible that pornography accessed in this way could desensitise people to, and normalise, extreme and harmful sexual behaviours. As these are nascent technologies, further ethically conducted research is needed.

A holistic approach to minimising harms to children from AI

The following list outlines possible regulatory and industry responses for mitigating AI harms to children:

- Various technical interventions to combat harms such as AI-generated child sexual exploitation and abuse, disinformation, and fraud. This includes tools to detect AI content and the use of watermarks on AI-generated images[310] and clear policies on AI-generated content and proactive enforcement of these policies.[311]
- Moving from principles to practice.[312] Governments, intergovernmental bodies and civil society have contributed to a growing collection of voluntary ethical principles, to help guide the safe application of AI.[313] However, more action in implementation is needed -

[308] M Elias, '*A deepfake porn scandal has rocked the streaming community. Is Australian law on top of the issue?'*, The Feed, 9 February 2023. https://www.sbs.com.au/news/the-feed/article/a-streamer-was-caught-looking-at-ai-generated-porn-of-female-streamers-the-story-just-scratches-the-surface/vfb2936ml

[309] B Helm, '*Sex, lies, and video games: Inside Roblox's war on porn*', Fast Company, 2020. https://www.fastcompany.com/90539906/sex-lies-and-video-games-inside-roblox-war-on-porn; S Pettifer, E Barrett, J Marsh, K Hill, P Turner and S Flynn, *'The future of extended reality technologies, and implications for online child sexual exploitation and abuse',* University of Manchester, 2022. https://documents.manchester.ac.uk/display.aspx?DocID=62042.

[310] W Knight, *This Uncensored AI Art Tool Can Generate Fantasies—and Nightmares*, Wired, 2022. https://www.wired.com/story/the-joy-and-dread-of-ai-image-generators-without-limits/.

[311] K Wiggers, *Deepfakes for all: Uncensored AI art model prompts ethics questions,* TechCrunch, 24 August 2022. https://techcrunch.com/2022/08/24/deepfakes-for-all-uncensored-ai-art-model-prompts-ethics-questions/?guccounter=1

[312] K Wiggers, *How new regulation is driving the AI governance market*, Venture Beat, 25 August 2021. https://venturebeat.com/ai/how-new-regulation-is-driving-the-ai-governance-market/.

[313] B Gocklin, *Guidelines for responsible content creation with Generative AI*, Contently, 3 January 2023, https://contently.com/2023/01/03/guidelines-for-responsible-content-creation-with-generative-ai/; Partnership on AI, *Responsible practices for synthetic media*,. https://syntheticmedia.partnershiponai.org/.

the European Union's Artificial Intelligence Act being one example of principles transitioning into practice.[314]

- In Australia, the Department of Industry, Science and Resources is currently leading consultation on establishing the safe and responsible use of AI.[315] This builds on the recent *Rapid Research Report on Generative AI* produced the National Science and Technology Council.
- Testing and monitoring AI applications throughout the system's full lifecycle, including post-deployment, through measures like auditing and transparency reports.
- Consideration of how the Act applies to generative AI and its integration into a range of online services. The Act is to be reviewed by January 2025.[316]

Decentralised online environments and tools

Decentralisation of the internet refers to distributing the control of the online data, information, interactions and experiences of users. Users and communities are said to have more power over their online experience because they can access online services and platforms without relying on a concentration of large technology companies.

Decentralised services have received increasing attention for their potential to enhance principles like transparency, privacy and data ownership. In late 2022, following Elon Musk's takeover of Twitter, many of its users created accounts on Mastodon, an open-source federated network that runs on independent servers.[317]

Bluesky, a project steered by former Twitter CEO Jack Dorsey, is working on developing an open and decentralised standard for social media. Bluesky is still in its early stages but has signalled an approach to content moderation which enables user and communities to decide how content is served and how feeds are curated.[318] Bluesky envisages developing an open-source standard which would allow many services like Twitter to be built using this standard. This common standard would enable different social media services to interact. In this environment, people would be able to choose a service which aligns with their content preferences, based on

[314] See: EU Future of Life Institute, *The Artificial Intelligence Act*, available at https://artificialintelligenceact.eu/.

[315] Department of Industry, Science and Resources, *Supporting responsible AI: discussion paper*, June 2023. https://consult.industry.gov.au/supporting-responsible-ai.

[316] *Online Safety Act 2021 (Cth),* s 239A.

[317] B Nolan and L Varanasi, *What is Mastodon and why are Twitter users flocking there? Here's everything you need to know*, Business Insider, November 2022. https://www.businessinsider.com/mastodon-twitter-users-flocking-elon-musk-social-meida-2022-11.

[318] K Main, '*Jack Dorsey's Bluesky Isn't Competing With Twitter. It's Surprisingly Future-Proofing It*', Inc. Australia, 2022, available at: https://www.inc-aus.com/kelly-main/jack-dorsey-bluesky-twitter-future-proofing.html.

the same underlying networks and data.[319] In theory, this could also enhance people's ownership of their data.

The potential movement towards decentralisation or web3 presents unique challenges to making sure online spaces are safe and age-appropriate. While a more decentralised internet could allow users to have more control over their online experience, it could also make it more difficult to hold users or services accountable for harmful content and activity. For example, eSafety administers its reporting powers through formal actions like content removal notices and informal requests to remove content. This requires communicating with platforms which have centralised authority to make moderation decisions and centralised stores of data. Given the potential absence of these centralised decision-making authorities, exercising content-removal regulatory functions could be far more difficult in decentralised spaces. eSafety's decentralisation position statement explores these issues in detail.

Decentralised services typically place a greater emphasis on community-led content moderation, given the lack of a centralised content moderation function. This could include community decisions on whether adult content is allowed, or minimum age requirements for members. Some centralised services also use community-based moderation, as it has the potential to reduce the scale of difficult content moderation decisions they must make. However, supporters of community-led moderation believe that it is a more democratic approach to moderation, as it allows users to set the standard of conduct and be accountable to one another (as it the case on Reddit).

Decentralised online communities may lack age assurance processes and robust moderation policies and enforcement outcomes. This can lead to greater inventories of adult content and higher chances of children encountering this content. Compounding this is the risk that decentralised services may more easily evade regulatory intervention, including efforts aimed at restricting underage access to online pornography.

The effectiveness of community moderation in decentralised environments is not yet well understood. Initial considerations for building safer decentralised services include enabling protocols which allow third party content moderation tools to function. For example, enabling protocols which permit tools that scan for pornography on services that prohibit it, alongside age assurance measures that prevent children from joining adult-focused communities.

[319] I Dodds, '*What is Bluesky, the potential Twitter alternative being tested by former CEO Jack Dorsey?*', *Independent*, 31 October 2022,. https://www.independent.co.uk/tech/bluesky-twitter-elon-musk-rival-b2213967.html.

Mastodon

Mastodon is a decentralised social network built on an open-source protocol which enables anyone to host an independent server.[320] Servers can choose their own content moderation policies, as long as they agree to follow the high-level overarching covenant[321] and minimum age requirements. Mastodon offers several features for users to control what they see and post, including the option to attach a content warning to posts[322] and to apply filters to automatically hide specific keywords and phrases. Reports of problematic content are sent to individual server moderators for decision based on that server's rules.[323]

Decentralised or self-sovereign identity

In our consultations, stakeholders discussed developments in relation to decentralised or self-sovereign identity (SSI) systems, and how they might helpfully contribute to age assurance efforts.

Contemporary digital identity systems include common centralised models, which require a unique username and password to access a service, and federated models where people can login into new services using their existing accounts, such as Google or Facebook accounts.[324] These systems have various benefits and drawbacks, including the risk that login and other personal information stored on centralised servers could be stolen or leaked.

SSI has emerged as a potential solution to these issues. It provides a way for people to control and manage their own digital identity through a decentralised system, instead of it being controlled by a third-party entity, such as a government or corporation. In the context of accessing pornography, an SSI or a decentralised identity could allow users to prove they are of a legal age when accessing pornography without disclosing other personal details such as their name, contact details, or date of birth.

SSI can be understood as a digital wallet that a person uses to store and manage their identifying information, such as their name, age, and other personal information. While widely used wallet services like Apple Pay and Google Pay can store credit cards, SSI goes beyond this by giving people ownership over their digital identifiers or credentials.[325]

[320] Mastodon, *We develop Mastodon*, 2023 https://joinmastodon.org/about.
[321] Mastodon, *Mastodon Server Covenant*, 2023. https://joinmastodon.org/covenant.
[322] Mastodon, *Posting to your profile*, 2023. https://docs.joinmastodon.org/user/posting/#cw.
[323] Mastodon, *Dealing with unwanted content*, 2023. https://docs.joinmastodon.org/user/moderating/.
[324] S Hori, *Self-sovereign identity: The future of personal data ownership?* World Economic Forum, 2021. https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership.
[325] L Newman, *Microsoft's Dream of Decentralized IDs Enters the Real World*, Wired, 2021. https://www.wired.com/story/microsoft-decentralized-id-blockchain/.

Generally, the starting point for such a system is an authoritative source such as a government passport office issuing credentials to a person's digital wallet. Then an online service, such as a pornography site, can interact with a person's digital wallet to seek confirmation they are over 18. When a person is asked to present a credential or attribute like their age, they can verify the credential belongs to them using cryptographic keys such as pin codes or biometrics (for example, a phone's Face ID).[326]

Distributed ledgers like blockchains can play a role as they form the network on which cryptographic hashes of actual identity is stored.[327] This provides the person with control over who to share their digital identity with and when, saving them from unnecessarily revealing extraneous personal information from a single identifying document.[328]

These identifiers can also be globally portable by adhering to technical decentralised identity standards, such as those developed by the World Wide Web Consortium.[329] SSI can also reduce privacy and security risks, such as services being targeted for cyber-attacks and other parties without permission, accessing sensitive data stored on central servers.

SSI Rollout

SSIs are currently being rolled out by major tech companies. For example, in September 2021, Microsoft launched its Azure Active Directory, which is a cloud-based identity and access management service. This allows users to control identifiable information from documents such as university transcripts, diplomas and professional credentials, and link with the Microsoft Authenticator app.[330]

Self-sovereign and decentralised identities are still being developed for mainstream use and it is uncertain when or if they will be implemented widely. Some stakeholders we consulted with felt these technologies held tremendous promise in the short-term; others were more sceptical and felt some aspects may be over-hyped. Broader digital identity developments within Australia are discussed in chapter 9.

[326] Microsoft Security, *Decentralized identity and verifiable credentials: Ownership, control, and trust for a digital world*, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5cxkr?culture=en-us&country=us.

[327] L Mearian, *Microsoft wants to use blockchain to secure your identity*, Computerworld, 2018. https://www.computerworld.com/article/3254774/microsoft-wants-to-use-blockchain-to-secure-your-identity.html.

[328] Jared Hanson, *The Keys to Decentralized Identity,* Okta, 2021. https://youtu.be/gWfAIYXcyH4?si=Wkkqq6NUjk3zez0c.

[329] A Giannopoulou, *Data protection compliance challenges for self-sovereign identity*, in J Prieto, A Pinto, A Das and S Ferretti (eds), Blockchain and Applications*. BLOCKCHAIN 2020,* Springer, DOI: 10.1007/978-3-030-52535-4_10.

[330] Newman, 2021.

Immersive technologies and the metaverse

While there is no single definition on what the metaverse is, it is commonly agreed that it will consist of networks of 3D virtual spaces where anyone can interact at the same time and maintain a continuous identity. This vision is likely to depend on the continued development of immersive technologies, such as headsets.[331]

If the major platforms achieve a degree of interoperability, the metaverse could become one, extended three-dimensional (3D) world. While interoperability could enable a frictionless experience, allowing users to maintain important settings like age attributes and safety preferences, it could also enable those who engage in harmful behaviour to seamlessly move across immersive environments. Safety must be considered as interoperability is designed.[332]

Or a metaverse could look more like a multiverse with a range of 'walled garden' offerings. Another scenario is where the spatial web is built on blockchain technologies, as part of a decentralised internet, or web3. What we do know is that the emergence of a metaverse – enabled by immersive technologies – has great potential to impact the way people learn, communicate, create and experience using new and emerging technologies.

These immersive technologies include augmented reality (AR), virtual reality (VR), mixed reality (MR) and experimental technologies like haptics and devices which stimulate your sense of smell, touch or event taste. Although haptic suit prices are currently out of reach for most of today's consumers, their promise of a full-body sensory experience adds another important dimension to the virtual experience.[333] The additional dimensions these technologies impose on experiences of online pornography mean it is critical that safety is built into metaverse governance to embed harm minimisation design and practices.[334]

Existing immersive environments and games

While we do not yet know what a metaverse or metaverse environments could eventually become, there are platforms that exist today which offer early insights.

An early market for immersive technologies is gaming, including platforms targeted to and popular among children and young people, such as *Fortnite, Minecraft, Rec Room, Roblox and*

[331] M Ball, *Framework for the Metaverse*, 2021. https://www.matthewball.vc/all/forwardtothemetaverseprimer.
[332] World Economic Forum, *Interoperability in the Metaverse,* World Economic Forum, 2023. https://www.weforum.org/reports/interoperability-in-the-metaverse/.
[333] eSafety Commissioner, *Gift guide – Haptics*, eSafety website n.d. https://www.esafety.gov.au/parents/resources/gift-guide/haptics.
[334] The Institute of Engineering and Technology, *Safeguarding the metaverse*, 2022. https://www.theiet.org/impact-society/factfiles/information-technology-factfiles/safeguarding-the-metaverse/.

VRChat. Although these platforms have policies prohibiting sexually explicit content,[335] there are reports of young children encountering sexual material and experiencing inappropriate interactions on immersive gaming platforms.[336] Pornhub's *2022 Insights Report* provides an outline of access rates through gaming consoles and breaks down searches of gaming characters from popular games like Fortnite.[337] The metaverse could allow people to expand on conventional online pornography by allowing users' avatars and AI-powered virtual characters engage in sexual acts.

There are also some immersive platforms which do allow pornographic elements.[338] For example, *BaDoinkVR* is a platform specifically for VR pornography. In addition, VR games such as *Dead or Alive 3* mix sexual elements with the option for users to act out harmful behaviours and gendered violence, particularly against women.[339] The gamification of violence against women is not new, and has long been a feature of popular games such as *Grand Theft Auto*, through which players can approach non-player character sex workers for implied sexual activity and then inflict violence or murder on them.[340] What is new is the heightened experience of interacting with digital content in 3D in ways that look, sound, and feel almost real – an effect described as 'hyper-realistic'.[341] Some people suggest virtual experiences will eventually be almost indistinguishable from physical experiences, while others point to the numerous technical barriers that still prevent this from happening.[342]

Safety measures in immersive environments

Services providing immersive environments have developed a range of features to minimise the risk of harm, including in relation to sexually explicit content and behaviour.

[335] Epic Games, *Content guidelines*, 2021, available at: https://www.epicgames.com/site/en-US/content-guidelines; Xbox, *Community standards for Xbox*, 2023, available at: https://www.xbox.com/en-AU/legal/community-standards; Rec Room, *Terms of service – Code of conduct*, available at: https://recroom.com/code-of-conduct; Roblox, *Community standards*, available at: https://en.help.roblox.com/hc/en-us/articles/203313410-Roblox-Community-Standards; VR Chat, *Community guidelines*, 2023, available at: https://hello.vrchat.com/community-guidelines.

[336] Epic Games, *Content guidelines*, 2021; Xbox, *Community standards for Xbox*, 2023; Rec Room, *Terms of service – Code of conduct*; Roblox, *Community standards*; VR Chat, *Community guidelines*, 2023.

[337] Epic Games, *Content guidelines*; Xbox, *Community standards for Xbox*, 2023; Rec Room, *Terms of Service – Code of conduct*; Roblox, *Community standards*; VR Chat, *Community guidelines*, 2023.

[338] J Ried, *VR game includes harassment feature*, The New Daily, 2016, available at: https://thenewdaily.com.au/life/tech/2016/09/05/dead-or-alive-sexual-assault/.

[339] M Carter and B Egliston, *'Ethical implications of emerging mixed reality technologies*', University of Sydney Socio-Tech Futures Lab, 2020 DOI: 10.25910/5ee2f9608ec4d, available at: https://ses.library.usyd.edu.au/handle/2123/22485.

[340] S Cole, *This Researcher studied how sex workers are portrayed in video games*, Vice, 2018, available at: https://www.vice.com/en/article/kzkv9v/sex-work-in-video-games-grand-theft-auto-v-fallout-new-vegas-sleeping-dogs.

[341] D Kaur, *Extended reality – Visualizing the future workplace*, TechHQ, 2020, available at: https://techhq.com/2020/12/extended-reality-the-technology-of-the-future/.

[342] J Murray, *'Virtual/reality: how to tell the difference',* Journal of Visual Culture, 2020, 19(1):11–27, DOI: 10.1177/1470412920906253.

Roblox

Roblox is a game-creation platform that allows users to design and play a wide variety of games. Their 'spatial voice chat' function allows users to hear the voices of other players in their proximity. Given the heightened risk this may present for inappropriate or harmful interactions between users of different ages, Roblox has instituted a minimum age of 13 to use spatial chat. This is verified through a process of matching an identity document with a selfie.[343]

This ensures there is a real user whose image matches their identity document. To protect user privacy, Roblox relies on a third party to store data in an encrypted form, and do not themselves store raw data from a user's ID.[344] Recognising that harmful content and conduct occurs despite the mandatory age verification, Roblox also enables users to mute, block and report breaches of their community guidelines.

While its age verification provides a high degree of certainty, there is a risk that younger users without government issued identification are excluded from accessing the feature.[345]

Meta Quest VR Headsets

Meta Quest has developed a series of VR devices that allow users to access immersive virtual gaming and entertainment spaces through an online account. Meta has introduced parental controls to their Quest headsets, allowing parents and carers to monitor and supervise a child's usage.[346]

Meta requires both the child (aged 13+) player and the parent to have Meta or Facebook accounts, and the Meta Quest app. The child must send an invite to the parent through the app to allow the parent to link their accounts and access parental controls. Once enabled, a child must seek permission from parents and carers to access apps that they are not old enough to use. Parents can also block specific apps, monitor screen time, view a child's friends, and be notified when they buy an app.

[343] Roblox, *Age ID verification*, available at: https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification.

[344] Roblox, *Age ID verification FAQs*, available at: https://en.help.roblox.com/hc/en-us/articles/4407276151188-Age-ID-Verification-FAQs.

[345] N Grayson, '*Roblox voice chat checks ID to keep kids safe, but slurs and sex sounds slip through',* The Washington Post, 16 November 2021, available at: https://www.washingtonpost.com/video-games/2021/11/16/roblox-voice-chat-id-requirement-slurs/.

[346] Meta, *Meta Quest – Parent education hub*, available at: https://familycenter.meta.com/au/our-products/quest/.

Heightened realism and impact

As virtual spaces become more realistic, there is concern that children may increasingly withdraw from their real-world relationships in favour of these online experiences.[347] In addition, hyper-realistic immersive environments may elevate common concerns that video games with violent and sexual themes encourage young people to replicate what they see online.[348]

While more studies are needed, there is some research suggesting that the illusion of VR is more effective on young children,[349] as well as those still developing the critical reasoning skills to distinguish real life events from those taking place in virtual environments.[350] VR is likely to evoke a stronger emotional response in children, including potentially longer lasting feelings of fear, anxiety and trauma, particularly in relation to highly graphic or violent content.[351]

Child-centric research on immersive environments

Children and young people are often early adopters of new technologies. It is critical that their voices are elevated to inform stakeholders on the guardrails needed for the spaces that they will be inhabiting.

Immersive technologies have the potential for many positive use cases for children and young people, yet it is important to recognise existing and emerging harms. eSafety's research shows that about 1 in 5 young people who have engaged in the metaverse said they experienced something that made them feel unsafe.

Recognising the need to understand young people's voices to proactively build a safe and inclusive metaverse, Meta funded Project Rockit to carry out youth consultations with 42 youth leaders. Participants came from a variety of backgrounds to account for diverse perspectives and vulnerable communities at a greater risk of encountering negative online experiences. The report details qualitative findings from the youth consultants, including the need for services to be designed with those most at risk in mind, and putting in place the right default settings for children.[352]

[347] N Reed and K Joseff, '*Kids and the Metaverse: What parents, policymakers, and companies need to know*', Common Sense, 2022, available at: https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf.

[348] Wassom, 2014.

[349] J Aubrey, M Robb, J Bailey and J Bailenson, '*Virtual 3eality 101: What you need to know about kids and VR*', Common Sense, 2018, available at: https://www.commonsensemedia.org/research/virtual-reality-101-what-you-need-to-know-about-kids-and-vr.

[350] B Kenwright, *'Virtual reality: Ethical challenges and dangers [opinion]'*, IEEE Technology and Society Magazine, 2018, 37(4):20–25, DOI: doi.org/10.1109/MTS.2018.2876104.

[351] Aubrey et al., '*Virtual reality 101: What you need to know about kids and VR*', 2018.

[352] L Thomas and E Unity, '*Our Metaverse: Young people and the digital future*', Project Rockit, 2022, available at: https://www.emilyunity.com/our-metaverse.

When determining the 'impact' of interactive computer games and films, the Australian Classification Board (Classification Board) is required to consider a range of factors, including - but not limited to - graphic and violent depictions and depictions of sexual activity. This ultimately determines what classification category, age restrictions and consumer advice an interactive game or film should be applied prior to its release to the Australian public.

The Guidelines for the Classification of Computer Games 2012 (the Guidelines) lists factors that heighten the impact of elements like sex and nudity. These include factors which immersive technologies could drastically enhance, such as content that:

- is highly interactive
- is realistic, rather than stylised
- contains greater detail, including the use of close-ups and slow motion
- uses accentuation techniques, such as lighting, perspective and resolution.

Variance in interactivity has an important effect on the viewer due to the differences between passively viewing compared to actively controlling outcomes by making choices to take or not take action. The Guidelines acknowledge that 'due to the interactive nature of computer games and the active repetitive involvement of the participant', that 'as a general rule' computer games will be classified higher than a film featuring similarly themed depictions. This is due to the greater potential for harm or detriment, particularly to minors.

This is particularly relevant to depictions of sexual activity and sexual violence. The perspective presented to the player may also create 'greater degrees of interactivity' (and therefore greater impact). This includes, whether the player is engaging from a first-person, third-person or top-down perspective. A VR game or other immersive experience is likely to enhance interactivity and take it to new levels.

Online safety education

It is important for online safety education and digital literacy efforts – including those in respect of online pornography – to keep pace with shifts in the technology ecosystem. Educational curricula must consider how new technologies, such as immersive devices and decentralised communities, are changing the way people interact with online pornography and the risks it may present to children. As the line between physical reality and hyper-realistic immersive environments blurs, education will play an important role in empowering young people to understand and mitigate the influence of online pornography in their lives.

Advancements in immersive technologies also offer opportunities to enhance education. Innovative forms of education taking place in metaverse environments could enable young people to experience and interact in new environments and experience historical events. They also offer children in rural or remote areas greater access to education and present opportunities for neurodiverse young people to socialise and learn in more accessible ways, opening space for dialogue on challenging and complex issues.[353]

eSafety's immersive technology gift guide provides parents and carers with practical guidance on keeping their children safe on the current range of VR devices and platforms available on the market.

Immersive pornography and sex tech

Given the potential to create a more intense and realistic experience, the sex tech and adult entertainment sectors have driven considerable innovation in immersive technologies.[354]

As immersive pornography matures, there is potential for it to be used in conjunction with other emerging technologies, further augmenting hyper-realism for users. This includes haptic suits and other wearables, which add tactile feedback to the immersive experience, as well as teledildonics, or internet-connected sex toys.[355] Adding physical sensation to visual and aural spaces can drastically increase the visceral impacts of a virtual experience, enabling users to feel more present with adult performers, partners, or NPCs, and boosting the connection between users and the content being viewed, felt, or touched.[356]

Other emerging technologies which could increase the level of interactivity with online pornography include holograms and AR enhancements. These technologies could enable the projection of and interaction with 3D representations of others, such as adult performers, into a person's immediate physical space.[357]

If designed with inclusivity and accessibility in mind, these technologies can generate a breadth of new opportunities and benefits, particularly for people with disabilities. They can also improve intimacy for people separated by distance. Yet, these technologies may also present new or enhanced risks. For example, commentators have raised the risk of sexual extortion where an immersive intimate interaction is recorded and threatened to be shared;[358] groping or sexual assault perpetrated through VR and haptics; [359] and rape by deception, where a person

[353] Thomas and Unity, '*Our Metaverse: Young people and the digital future*', 2022.
[354] B Marr, *Future of intimacy: Sex bots, virtual reality, and smart sex toys*, Forbes, 2020, available at: https://www.forbes.com/sites/bernardmarr/2020/11/30/future-of-intimacy-sex-bots-virtual-reality-and-smart-sex-toys/?sh=5a6ff00f38fa.
[355] R Sparrow and L Karas*, 'Teledildonics and rape by deception'*, *Law, Innovation and Technology*, 2020, 12(1):175-204, DOI: 10.1080/17579961.2020.1727097.
[356] N Döring, N Krämer, V Mikhailova, M Brand, THC Krüger and G Vowe, *'Sexual interaction in digital contexts and its implications for sexual health: A conceptual analysis'*, Frontiers in Psychology, 2021, 12, DOI: 10.3389/fpsyg.2021.769732.
[357] J Owsianik, '*The future of sex: How intimacy is transforming*', Futurism, 2017, available at: https://futurism.com/the-future-of-sex-how-intimacy-is-transforming.
[358] Sparrow and Karas, 2020.
[359] M Lemley and E Volokh, *'Law, virtual reality, and augmented reality'*, University of Pennsylvania Law Review*,* 2018, 166:1051 DOI:10.2139/ssrn.2933867.

may believe their intimate partner is controlling an experience, but it is actually a third party to whom consent was not given.[360]

Children face a range of potential harms, especially if age-based safeguards are not implemented. While outside the scope of this report, we note this includes risks in relation to the grooming, sexual exploitation and abuse of children by adults. The severity and breadth of these risks compounds the need to act. Accordingly, robust age assurance measures are likely to play a critical role in preventing a wide range of harms to children and ensuring they have the freedom to explore age-appropriate virtual environments safely. Age assurance will need to be accompanied by a range of other measures, including classification ratings, parental controls and information, effective and easy-to-use reporting and safety features, and proactive content and activity moderation.

Regulatory challenges due to blurred lines between online content, conduct and contact

The prospect of a widely adopted metaverse, accessed through immersive technologies, has the potential to significantly change where and how children encounter online pornography and to blur the lines between pornography, gaming and socialising.[361] It will also blur the distinction 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.

Given the legal age of consensual sex ranges from 16 to 17 in Australian states and territories,[362] the potential shift from consuming content to acting out conduct surfaces questions around minimum age restrictions for metaverse environments. As this age is lower than the age to view pornography, it is possible that immersive environments where users can engage in sex could have different age restrictions.

This shift is important from a regulatory perspective, as many of eSafety's current enforcement powers centre on being able to compel the removal of material rather than on harmful activity that creates material or causes the material to be livestreamed in real time. This is much harder to target. This highlights the importance of a Safety by Design approach, where services

[360] Sparrow and Karas, 2020.

[361] W Oremus, *'Kids are flocking to Facebook's 'metaverse.' Experts worry predators will follow'*, The Washington Post, 7 February 2022, available at: https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/; Center for Countering Digital Hate, '*Facebook's Metaverse*', 2022, available at: https://counterhate.com/research/facebooks-metaverse/; A Crawford and T Smith, *'Metaverse app allows kids into virtual strip clubs',* BBC News, 2022, available at: https://www.bbc.com/news/technology-60415317; C Fitzsimmons, 'Sometimes I experience nothing, other times it's rampant: sexual material warning on Roblox', 2021.

[362] Australian Institute of Family Studies, '*Age of consent laws in Australia*', 2021, available at: https://aifs.gov.au/resources/resource-sheets/age-consent-laws-australia.

assess potential risks upfront and build in preventative measures. This approach could be embedded in industry codes or standards which set out steps platforms would take to build safety by design into their systems and reduce the likelihood of harmful activity occurring.

Elements of the immersive technology stack are already covered by the current Act. For example, immersive devices and platforms may fall within the definitions of 'equipment',[363] 'social media services,'[364] 'relevant electronic service,'[365] 'designated internet service,'[366] or 'app distribution services.'[367] However, it will be important to consider whether eSafety's powers and the expectations and requirements that apply to these different sections of the online industry remain fit for purpose in immersive environments. For example, some forms of age assurance that may be proportionate for online pornography today, may be inadequate for the heightened intensity of live and interactive sexual interactions in immersive environments. eSafety encourages consideration of this issue in the upcoming review of the Act.

Content and activity moderation

Content and activity moderation efforts will remain critical to reducing the risk of children accessing pornography in evolving online spaces.

Currently, automated classifiers and predictive systems are widely used to detect illegal and harmful text or images, such as pornography on services where it is disallowed by the terms of services. These systems are likely to need significant modifications to adapt.[368]

In an immersive digital environment where live behaviour and conduct, rather than textual or visual content are the main forms of interaction, these automated tools may lose their utility.[369] More research and greater investment from industry is required to investigate how to moderate live and converging harms in virtual environments.

While developing and refining automated content moderated systems is essential, this needs to occur in conjunction with human moderation, as moderation algorithms can be prone to error and may fail to detect important contextual information. The unconstrained use of moderation algorithms can have a disproportionate impact on marginalised and minority groups, including adult performers and sex workers. It is

[363] Online Safety Act 2021 (Cth) s 134(h).
[364] Online Safety Act 2021 (Cth) s 13.
[365] Online Safety Act 2021 (Cth) s 13A.
[366] Online Safety Act 2021 (Cth) s 14.
[367] Online Safety Act 2021 (Cth) s 5.
[368] See Appendix 5.
[369] K Clark and T Le, '*Sexual assault in the Metaverse isn't a glitch that can be fixed*', Monash Lens, 2022, available at: https://lens.monash.edu/@politics-society/2022/10/13/1385033/sexual-assault-in-the-metaverse-isnt-a-glitch-that-can-be-fixed.

important that algorithmic content moderation does not arbitrarily restrict the online presence of these communities in spaces where it is lawful for them to operate.[370]

Privacy

There are also likely to be novel issues unique to a metaverse and immersive environments. These may relate to the unprecedented digital footprint created from using immersive technologies, which are perhaps the most data-extractive devices to be used in such personal and intimate circumstances.[371] There need to be requirements for industry to minimise the data collected and make sure users are aware of how their personal information may be used. This includes location information, biometric data such as eye movements or heart rate, and data on user preferences inferred through combining biometric information with predictive behavioural analytics. There is a risk of this information being stolen, shared or used to profile people in invasive new ways.[372]

It will be critical to balance the interrelated safety, privacy and security considerations associated with increased data flows. For example, while the collection and analysis of biometric data and behavioural analytics gives rise to privacy and security risks, this could also form an important source of data for confirming the age of young users – an essential step in keeping them safe. Common international standards for industry will be particularly important given these novel risks and the potential for immersive technologies to be integrated across a variety of sectors. Various initiatives are already underway, including, for example:

- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) joint technical committee on Health, Safety, Security and Usability of Augmented & Virtual Reality.[373]
- The IEEE Standards Association is also actively working on various immersive technology standards.[374]
- The XR Safety Initiative is a global, non-profit standards developing organisation that promotes privacy, safety, security, and ethics in immersive environments.[375]

[370] Z Stardust, E Nagel, K Tiidenberg, J Lee, E Coombes and M Miller-Young, '*Manifesto for sex-positive social media*', ARC Centre of Excellence for Automated Decision-Making and Society, 2022, available at: https://eprints.qut.edu.au/235033/; See Appendix 5.

[371] B Heller, *'Watching androids dream of electric sheep: Immersive technology, biometric psychography, and the law'*, Vanderbilt Journal of Entertainment and Technology Law, 2020, 23(1).

[372] Heller, 2020.

[373] iTeh Standards, '*ISO/IEC JTC 1/SC 24/WG 11 - Health, Safety, Security and Usability of Augmented & Virtual Reality (AR/VR)*', available at: https://standards.iteh.ai/catalog/tc/iso/8031adc3-c1a7-44a1-80a5-f817b7943f4c/iso-iec-jtc-1-sc-24-wg-11.

[374] IEEE Digital Reality, *Standards*, available at: https://digitalreality.ieee.org/standards.

[375] XR Safety Initiative, *Who we are*, available at: https://xrsi.org/who-we-are.

- The World Economic Forum (WEF) is also considering governance of metaverse environments through the establishment of the WEF Metaverse Governance Steering Committee.

Conclusion

Online safety technologies, including parental controls and age assurance measures, will be essential to reducing the risks to children associated with online pornography in the next iteration of the internet.

Any age assurance standard or accreditation scheme should be technology neutral so it can apply to emerging technologies and can accommodate interoperability and disruptions to the digital ecosystem, caused by shifts towards immersive or decentralised technologies. There are opportunities to build in device-level age assurance and filtering mechanisms as a minimum standard, by default. The Safety by Design principles (discussed in chapter 12) remain fundamental and provide a blueprint for a safer technologies and immersive environments.

Transparency and accountability remain hallmarks of a robust approach to user safety and should act as a catalyst for a race to the top in terms of user safety. Companies must be transparent about known risks with emerging technologies and in emerging environments. They must also disclose measures they are taking to address them – and they need to share data about the uptake and efficacy of these safety tools.

As the tech stack evolves, so too will thinking about reasonable, proportionate and effective steps that may be taken at each layer to prevent children from harms associated with online pornography. New technologies like generative AI give rise to new tech stacks. This raises important accountability questions where issues arise, such as how much responsibility for content generated lies with the end user, the operating system, or the data sets on which the systems are modelled.[376] In line with a holistic approach, wherever there is risk of children accessing or creating pornography, incorporating friction and safety messaging will help to minimise these risks.[377]

Where content is accessed incidentally, users should be empowered with real time friction points that allow them to put in place 'safe zones' and to mute, block and report content. At the same time, parents and carers should be empowered with appropriate tools and features that enable them to supervise the online experience of children in a proportionate way as they grow and mature.

[376] N Lomas, *Who's liable for AI-generated lies?*, TechCrunch, 2022, available at: https://techcrunch.com/2022/06/01/whos-liable-for-ai-generated-lies/.
[377] See Appendix 5.

Further research would support policymakers and regulators in understanding and mitigating harms to children that stem from how emerging technologies change the ability to access pornography and the nature of engaging in pornography.

eSafety next steps and Recommendations for the Australian Government

eSafety's next steps

- 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.
- 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 the tech 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.

Recommendations for the Australian Government

- 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 of and feelings of children and young people
    - What children and young people are learning from 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 risks groups, especially those that 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.

Part 3 – Technology based responses

This volume of the report outlines technology-based responses to preventing and mitigating harms to children from online pornography, including age assurance and other safety technologies. It assesses the risks and benefits of each technology, considers the necessary policy and regulatory settings and provides high level direction and considerations for industry.

Table of contents

Chapter 8: Age Assurance technology interventions

Key points

- There are many different methods for determining the age of users, including: the use of identity documents, techniques which estimate age based on a person's face or voice, and technologies which analyse online behaviour to determine a likely age range.
- Over 3 in 4 Australian adults surveyed as part of our public perceptions research support the implementation of age assurance technology by the Australian Government, to confirm users meet a minimum age to access online pornography.378 This is consistent with equivalent overseas research and findings from eSafety's research with young Australians (91%).
    - Some respondents expressed scepticism regarding implementation of mandatory age assurance, including effectiveness and the ability to safeguard privacy and security.[379] These concerns and additional views on accessibility, fairness and bias – were echoed in eSafety's research with 16-18-year-olds, stakeholder and Youth Council consultations.
- The age assurance industry and associated technologies are new and still evolving. Consideration of international standards, products tested against these standards, and allowances for user choice can empower individuals to choose a service that meets their privacy preferences and circumstances.
- eSafety developed a set of criteria to assess different categories of age assurance technology, based on the key factors which emerged in our research and consultations.
    - Using these criteria, Enex TestLab provided an independent assessment of technologies available on the market and reviewed the findings from recent age assurance trials conducted by euCONSENT in Europe.

[378] eSafety Commissioner, *Public perceptions of age verification for limiting access to pornography*, available at: https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography.

[379] eSafety Commissioner, Public perceptions of age verification for limiting access to pornography, available at: https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography.

- Enex TestLab suggested that age assurance technologies should be trialled in the Australian context before being prescribed, building on lessons learned through the recent euCONSENT pilot.
- 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. It 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 frameworks such as the Digital Transformation Agency's *Trusted Digital Identity Framework*.

Overview

Technologies have a role in limiting children's exposure to harmful content, but technological solutions alone cannot prevent children from accessing online pornography or other age-inappropriate content or services.[380] Consequently, eSafety was tasked with developing a multifaceted approach to preventing and reducing adverse effects to children from online pornography.

Against this backdrop, eSafety was asked to undertake 'detailed research as to if and how a mandatory age verification mechanism or similar could practically be achieved in Australia'.[381] This chapter sets out the process and findings of that research and consultation, analysing the existing age assurance measures available today.

There is a spectrum of measures which provide different levels of assurance. Consistent with insights from our stakeholder consultations and the Attorney-General's Department's consultation on the previous government's *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*[382], this chapter considers a range of age assurance measures (not limited to 'age verification'), including:

- age-gating based on age self-declaration
- account-based assurance (e.g., cross-authentication with another account)
- vouching for another person's age

[380] Australian Government, *Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence,* Parliament of Australia, 2021, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Government_Response, p 2.
[381] Australian Government, *Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence,* 2021, p.5.
[382] Attorney-General's Department, *Online Privacy Bill exposure draft*, 2021, available at: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.

- artificial Intelligence (AI) profiling or inference models that estimate age on behaviour
- using biometrics and capacity testing to estimate age based on characteristics or aptitude
- requiring 'hard identifiers' such as government-issued identity documents (ID) or digital versions of these documents, or drawing on new developments in the field of digital identity.

These measures are not mutually exclusive and multiple measures may be applied by a single service. For example, a social media service may apply age gates based on users' self-declared age, but also employ AI profiling and user reporting mechanisms to detect potential underage accounts (for example, Facebook currently uses these methods)[383]. This may result in an account being suspended until the user verifies their age by providing a hard identifier, such as government ID.

In preparing this report, eSafety consulted with stakeholders within the online industry about their current and emerging approaches to age assurance and maintained a watching brief on new developments. This revealed a clear trend towards greater uptake of age assurance and complementary measures by social media and other online services to prevent a range of harms to children, including but not limited to preventing their access to online pornography. However, significant gaps remain, particularly on pornography-specific services.

Efforts to prevent, detect and remove underage users may also be supplemented with various content detection and moderation measures, as well as tools for users to exercise greater control over the content they see, as discussed in chapter 11.[384] Increasingly, industry is adopting these measures to prevent a range of harms to children.

This chapter re-visits eSafety's consultation and research methodology outlined in chapter 3, exploring public perceptions of age assurance, and identifying some of the challenges and tensions government should consider prior to mandating any age assurance regime in the Australian context. It then assesses common categories of age assurance, as well as some specific products, against criteria shaped by stakeholder consultations and our research.

All assessed products are provided by third-party vendors for integration into a variety of online services. The use of a trusted and accredited third-party provider can bolster privacy and security, particularly in double-blind systems where the underlying online service does not

[383] Meta, *How Facebook knows an app user is old enough*, 2021, available at: https://about.fb.com/news/2021/07/age-verification/.

[384] Twitch is an example of a service which combines these measures to prevent under 13s from having accounts to reduce the risk of online grooming and other harms. See: Twitch, *Our ongoing work to combat online grooming*, 2022, available at: https://safety.twitch.tv/s/article/Our-Work-to-Combat-Online-Grooming?language=en_US.

receive any information about the identity of the user and the age assurance provider does not record which online services the user is accessing.

This chapter discusses a recent double-blind age assurance pilot conducted in Europe. Building on this analysis, chapter 9 discusses how age assurance mechanisms may be tested and implemented considering broader ongoing developments in relation to digital identity, international standards, and the legislative and policy environment in Australia.

Terminology

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.

Age tokens are re-usable electronic ‘tokens’ that carry an age attribute once a person’s age has been verified or estimated. Rather than providing a user’s specific age, these tokens can be limited to confirming that a user does or does not meet a minimum age requirement.

Age verification measures determine a person’s age to a high level of certainty, while age estimation technologies provide an approximate age or age range. 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.

Biometrics for age assurance analyse a person’s characteristics, such as their face or voice, to estimate their age.

Cookies are small pieces of data from a web site that is stored on a visitor’s device and processed and stored by browsers to help websites track the visitor’s activity.

Digital wallet the app or software which allows users to store or share attributes of their digital identity. It offers users control over which attributes they share and for how long.

Double-blind systems allow for a user’s age to be confirmed without the age assurance provider seeing which age-restricted online service a user is accessing, and without the online service seeing any personal information the provider used to confirm the user’s age.

Hard identifiers are a very accurate age assurance method, particularly when paired with liveness checks. Hard identifiers are often used for offline age-restricted goods and services. Hard identifiers can be used to verify a person's age either through viewing the physical version of a document, uploading a copy for its details to be extracted and validated using optical character recognition and verification against an existing database.

Zero-knowledge proof a method based on a process in cryptology that allows individuals to prove their age without having to reveal any other information.

Research, consultation and third-party assessment

Primary research

eSafety conducted an online survey of 1,200 adults living in Australia in early 2021 to better understand people's awareness and acceptance of age verification systems for preventing children's access to online pornography.[385] While 70% of respondents displayed unprompted awareness of 'identity verification,' only about half (51%) were aware of 'age verification,' dropping to 18% awareness of 'age estimation' and 5% awareness of 'age gating.'

Once these concepts were explained, more than three quarters (78%) supported the implementation of age verification technology by the Australian Government to verify a minimum age to access online pornography. This is consistent with research commissioned by Ofcom and the Information Commissioner's Office in the UK, which found most parents felt services should have age assurance measures.[386] Parents also felt these measures were most appropriate for activities associated with age restrictions offline – such as gambling, buying alcohol and watching pornography.

> 'I do agree that whether the pornography is offline or online it should have the same age-based restriction' – Adult public perceptions of age verification survey participant.
>
> 'I think it is necessary, but I would worry who would be asking for verification and if they would exploit it' – Adult public perceptions of age verification survey participant.

[385] eSafety Commissioner, *Public perceptions of age verification for limiting access to pornography*, available at: https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography.

[386] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022, available at: https://www.gov.uk/government/publications/families-attitudes-towards-age-assurance-research-commissioned-by-the-ico-and-ofcom.

Notably, 24% of respondents said they lacked confidence in the design, implementation and operation of an age verification system. Specific issues highlighted by respondents included: the potential for users to lie and bypass the system (28%), concerns about data security and identity theft (17%), and the privacy of personal information (6%).

These same concerns emerged in eSafety's research with young people aged 16-18 and in consultation with the eSafety Youth Council. Participants in the youth survey and focus groups generally supported age-based restriction of online pornography. However, many thought age verification methods could be easily circumvented and were concerned about privacy and data security. Of those surveyed, 91% of young people had concerns about the specific age assurance approaches suggested during the research process. Specifically, 63% were concerned about the 'privacy of personal information' and 58% were concerned that 'people could lie or bypass the [age assurance] system'. When discussing different ways to verify age online, members of our Youth Council also frequently raised concerns about the privacy and security of methods, and the perceived ease of circumventing many methods.

About one in three participants thought '*providing an official government document e.g. a driver's license*' (35%) and *'stating your year of birth'* (30%) were appropriate ways for people to provide evidence they are the legal age to access online pornography. One in five (20%) were unsure of the appropriate ways to provide evidence.

> 'I can't think of any way the restriction could be implemented without massive privacy concerns. Even if some super strict id verification processes were needed, there would be mirror sites popping up without the same requirements' – eSafety focus group participant, 18
>
> 'I think restrictions on pornography consumption will have no effect. People will find ways to bypass it' - eSafety focus group participant, 17

Consultation and call for evidence

In August 2021, eSafety issued a call for evidence to better understand age verification techniques, the impact of online pornography on children, and proven methods of educating young people about both respectful and harmful sexual behaviours. A thematic analysis of the evidence and insights from this process is available on the eSafety website and in **Appendix 2**. Key suggestions in relation to technology included:

- Any online service provider that poses a risk of exposing children to pornography should have measures in place to prevent children gaining access.
- A specific age assurance tool should not be prescribed. Instead, there should be a range of potential technological tools available which are certified and independently

audited to make sure they meet strict safety and privacy standards. The role of filtering and parental controls should also be considered.

- A one-size-fits all technological solution would not be effective. Technological requirements should be proportionate and based on risk.
- Industry should design technologies so they are easy for children and parents to understand. Information on how the technologies work and how they use, store, and protect data should be readily available.
- Technologies employed to prevent children from accessing online pornography should not have the effect of blocking adolescents' access to sexuality and sexual health information or restricting adults' lawful access to online pornography.

Following the call for evidence, eSafety held stakeholder consultations with a diverse range of organisations and individuals.[387] Stakeholders highlighted a range of technologies for consideration. They also raised a variety of concerns about the accuracy and effectiveness of different technologies; their cost and the potential impacts on smaller businesses and competition; the accessibility of these technologies across user groups and their potential for bias or exclusion; and concerns about privacy.

Independent assessment

To supplement and strengthen this research and consultation, eSafety asked Enex TestLab to provide an analysis of relevant international standards and to review the findings from recent age assurance trials held in Europe. Enex TestLab also conducted an independent assessment of various age assurance and safety technologies shared with eSafety throughout the consultation process, using a set of criteria developed by eSafety. Enex TestLab's report is attached at **Appendix 8**. The technologies discussed in the report include:

Age assurance (using biometrics and hard identifiers to determine age)	• AgeChecked • Ageify • Mastercard ID	• Privately • Yoti
Content Moderation (using AI to detect and action content such as pornography)	• Spectrum AI	
Content filters (using content patterns to identify and block certain content, such as pornography)	• ASUS ZenWiFi Pro XT 12 • McAfee Safe Family • McAfee Secure Home Platform • Norton Family	

[387] For consultation summaries, see Appendix 5. For a list of consultation participants, see Appendix 6.

Assessment criteria

eSafety developed its assessment criteria by identifying the key issues raised in our consultation process and our primary research. For consistency and comprehensiveness, these issues were mapped against existing criteria and frameworks used to assess age assurance technologies, including those applied by 5Rights, UNICEF, and the Internet Safety Technical Taskforce.[388]

Our assessment criteria consist of both design and implementation factors, for example, the type of data it requires to assess age (design) and whether its use is supported by transparent governance and compassionate appeals processes (implementation). The assessment was limited by time constraints and a lack of available information from some vendors. As technologies are not yet widely implemented, assessment of implementation factors has been challenging. Additionally, there are only a small number of providers within each product category, limiting the ability to compare different products.

This chapter primarily focuses an assessment of design factors. Where Enex TestLab and eSafety could access information on implementation factors, they are also considered. Some of these factors, such as transparent decision-making, can be assessed against a particular technology product or the way its provider operates. Others, such as independent oversight to make sure compliance with privacy, security and human rights, can only be assessed against the broader context and enabling environment in which the providers exist and the technologies are applied.

Enabling environment factors are also discussed in chapter 9, against the backdrop of the many intersecting legislative and policy developments within Australia, including the Trusted Digital Identity Framework and the Privacy Act review. These developments inform eSafety's recommendations to government.

Design factors considered 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

[388] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021, available at: https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html; Internet Safety Technical Task Force, '*Enhancing child safety and online technologies';* UNICEF, *Digital age assurance tools and children's rights online across the globe: A discussion paper*, 2021; Berkman Centre for Internet & Society, *Enhancing child safety & online technologies: Final report of the Internet Safety Technical Task Force,* Harvard University, 2008, available at: https://cyber.harvard.edu/pubrelease/isttf/.

- 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 considered at the product or provider level and/or the enabling environment level 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
- proportionality to the risks of harm based on the available evidence, as outlined in chapter 5.

Age assurance technologies

There are a range of age assurance technologies which carry different benefits, challenges and trade-offs in relation to effectiveness, certainty, accessibility, inclusivity and privacy. These age assurance measures can be used on their own, in combination with other age assurance measures, and/or as part of a broader suite of safety measures. In addition, they may be deployed by a specific online service or by a third-party provider. It is important to note that age assurance is not identity verification. While many technologies offer the ability to verify age and identity, a user's identity does not need to be verified to determine they are old enough to view online pornography.

This chapter considers age assurance technologies across several contexts, reflecting the potential for age assurance to protect the rights of children (such as exemptions from data collection) and support them to have safe and age-appropriate experiences online. It also highlights that age-inappropriate content, such as online pornography, can be accessed by children on a range of services, not just online pornography sites.

Age assurance technology in use

In the 12 months leading up to the submission of the roadmap to the Australian government in March 2023, Google, Meta and Yubo (among others) made announcements about the use of age assurance technology on their services, reflecting a trend towards the uptake of age assurance measures across industry.

At the time of this report, current age assurance measures in place include:

- YouTube users in Australia can confirm their age to view age-restricted content by providing credit card details or a copy of a valid government ID.[389]
- Social media platform, Yubo, has partnered with Yoti to check the age of their users using age estimation technology.[390]
- Instagram users have the option to verify their age on Instagram using a range of methods, including government ID and Yoti's age estimation technology. Testing for this option was expanded to Australia in March 2023.[391]

[389] Google, *Access age-restricted content & features*, available at: https://support.google.com/accounts/answer/10071085

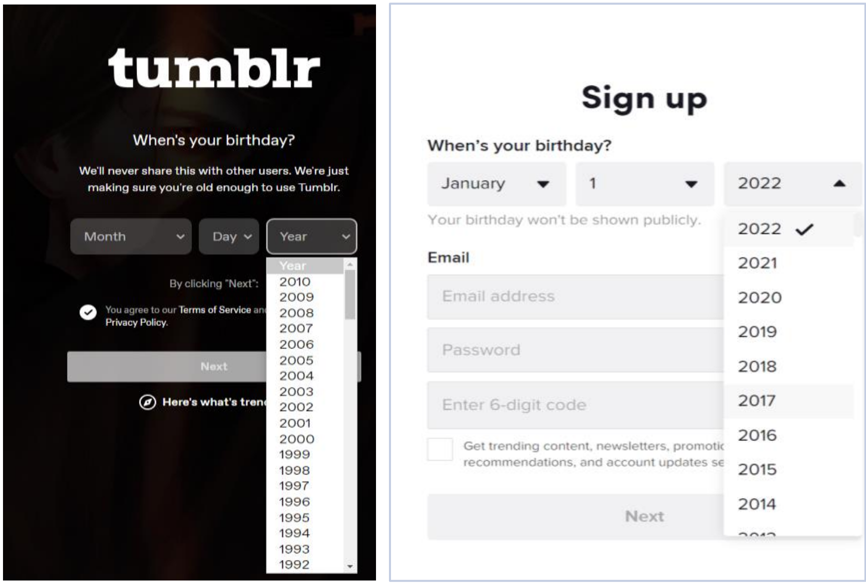
[390] Yubo, *Yubo's new age verification feature helps keep you safe*, 2022, available at: https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe.

[391] Meta, *Introducing new ways to verify age on Instagram*, 2022, available at: https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram.

- Roblox users can verify their age using government ID to access certain age-restricted parts of the service, such as spatial chat.[392]
- OnlyFans users and creators need to confirm that they are over 18 to use the platform. OnlyFans uses a combination of age assurance technologies and approaches. In some countries (not including Australia), users (fans) can use age estimation technology to satisfy account requirements, while creators (who produce and share content) must undertake rigorous age verification processes to confirm their age and identity.[393] This process may include age verification using hard identifiers.

Age gating based on self-declared age

Self-declaration is where a user states their age but does not provide any evidence to confirm it.[394] This could involve asking a person to tick a box indicating they are over a particular age or requiring them to enter their age or date of birth. If they identify as being under the relevant age, an age gate prevents them from accessing the service or particular content on the service.



tumblr

When's your birthday?

We'll never share this with other users. We're just making sure you're old enough to use Tumblr.

By clicking "Next":

You agree to our Terms of Service an Privacy Policy.

Sign up

When's your birthday?

January 1 2022

Your birthday won't be shown publicly.

Email

Email address

Password

Enter 6-digit code

□ Get trending content, newsletters, promotic recommendations, and account updates se

Figure 6 Examples of self-declaration. The Tumblr form only allows users to enter birthdates that meet age requirements while Tiktok allows users to enter younger birthdays (submissions under 13 mean accounts cannot be created.

[392] Roblox, *Age ID verification – Roblox Support*, Roblox website, available at: https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification.

[393] Yoti, *How OnlyFans became the first UK subscription-based platform to protect children and create age-appropriate experiences*, 16 June 2023, available at: https://www.yoti.com/blog/how-onlyfans-became-the-first-uk-subscription-based-platform-to-protect-children-and-create-age-appropriate-experiences/.

[394] UK Information Commissioner's Office, *Age Appropriate design: A code of practice for online services - 3. Age appropriate application*, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/.

Level of assurance

Relying on users to declare their age voluntarily is not considered a reliable or accurate method of age verification, though it is the measure most often used on social media.[395] Recent Ofcom-commissioned research found 32% of UK children aged 8-17-years-old have a social media account with a self-declared user age of 18 or above, and 47% of children aged eight to 15 have a user age of 16 and over on their social media accounts.[396] Similarly, Australian research asked 1500 Australians aged 16 and over whether self-declaration[397] was effective; 82% of respondents said it was not and 59% supported stricter confirmation of age.[398]

Age gates supported by self-declaration can be implemented in several ways. Some services allow users to enter any date, up to and including the current date. Others provide cut offs which prevent a user from entering a birthdate that would be too young (see Figure 6 comparison of Tumblr and TikTok sign-in screens). Although some services allow users to subsequently enter a different birthdate if their initial response results in access being denied, services such as TikTok prevent users from doing so by using persistent cookies. In our consultations, stakeholders told us it is considered 'better practice' to ask a user to enter their date of birth, instead of having them tick a check box or providing a pre-filled form with the requisite age as the latter options were considered more likely to lead to false responses. They also highlighted that if a user enters a birthdate which suggests they are too young to use the service, the platform should not allow the user to immediately re-enter a different birthdate.[399] Similarly, services can consider asking users to re-enter their birthdate again at later stages of sign-up – or after a period of time – to confirm it was correct, as those who entered a false birthdate may not remember the date they provided. However, a false birthdate is not always indicative of an under-age user; some users may provide false details because they do not trust services with their personal information.

Feasibility and effectiveness

Self-declaration of age is an extremely common, low-cost and low-effort method to ascertain a user's age and it is also easy to circumvent.

The age gate does not present a high barrier for access, but it is important to acknowledge that it can 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

[395] Age Verification Providers Association (AVPA), '*International standards for age verification*', available at: https://avpassociation.com/standards-for-age-verification/.

[396] Ofcom, '*Children's Online User Ages Quantitative Research Study*', 2022, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart-pack.pdf.

[397] Respondents were asked whether 'common arrangements that ask website or app users their age or date of birth before granting access' were effective.

[398] Resolve, '*Consolidated industry codes of practice for on-line class 1 content: Community research (Commissioned by Digital Industry Group Inc and Communications Alliance')*, Online Safety, 2022, available at: https://onlinesafety.org.au/submissions/

[399] See Appendix 5.

users to confirm that they wish to pass the age gate to enter the website and see the content. 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 where users make a conscious decision to continue. This can reduce unintentional and unwanted encounters by deterring some children from proceeding to view the content.

Accessibility, barriers to inclusion and potential for bias

There are few barriers to inclusion, other than a hesitancy or unwillingness among some users to share their date of birth with the service. Depending on the design of the website, it may also pose challenges to users with assistive technology. A benefit to this option is its minimal potential for bias in decision-making. Stakeholders did not raise concerns about potential bias to eSafety during consultations.

Sensitivity of data

While a birthdate can be used to identify a person, and therefore may be 'personal information', it is not 'sensitive information' as defined in the Privacy Act.[400] However, recent UK research shows some users are hesitant to share this information with online services:

> 'One father of a 16-year-old boy talked about, as a family, not being honest about their dates of birth online. He had told his children to state the actual year they were born but an incorrect day and month, as he did not want their children's information to be available online'. [401]

Overall assessment of self-declaration of age

With a low level of assurance, Enex TestLab found self-declaration an unacceptable verification or validation of age on its own. Self-declaration of age may be suitable for low-risk services or in conjunction with other methods.

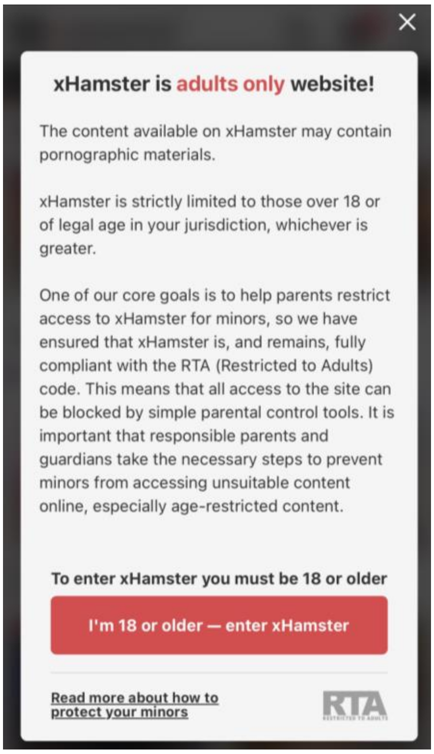
Similarly, 5Rights Foundation has assessed self-declaration as suitable only for low-risk products which do not include features that impact negatively on children. The low friction experience may prevent children from understanding the impacts of pretending to be older on

[400] Section 6 of the *Privacy Act 1988* (Cth) defines sensitive information as information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information about an individual that is otherwise not health information, biometric information that is to be used for the purpose of automatic verification or biometric identification or biometric templates.

[401] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

their user experience.[402] eSafety was not able to assess the effectiveness of self-declaration for different developmental stages. However, this may be a suitable area of future research.

Age self-declaration can be effective in preventing unintentional access, particularly where children are aware of what online pornography is and want to avoid it but have accessed a site hosting online pornography (either through mistakenly following a link or being sent a link to the material).



xHamster is adults only website!

The content available on xHamster may contain pornographic materials.

xHamster is strictly limited to those over 18 or of legal age in your jurisdiction, whichever is greater.

One of our core goals is to help parents restrict access to xHamster for minors, so we have ensured that xHamster is, and remains, fully compliant with the RTA (Restricted to Adults) code. This means that all access to the site can be blocked by simple parental control tools. It is important that responsible parents and guardians take the necessary steps to prevent minors from accessing unsuitable content online, especially age-restricted content.

To enter xHamster you must be 18 or older

I'm 18 or older — enter xHamster
Read more about how to protect your minors
RTA

Figure 7 Pop-up age gate for first time visitors to pornography website xhamster.com

Platforms and services which use age-gating (non-exhaustive list)

- Facebook
- TikTok
- Discord
- Instagram
- Twitter
- xHamster –the only pornography website out of the top five most accessed porn sites from Australia to include an age gate. This age gate only pops up on the first access to the website and simply requires the user to click a button which states *'I'm 18 or older'*. Once this button is clicked users are directed to the home page which contains numerous uncensored pornographic videos.

[402] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021.

Account-based assurance

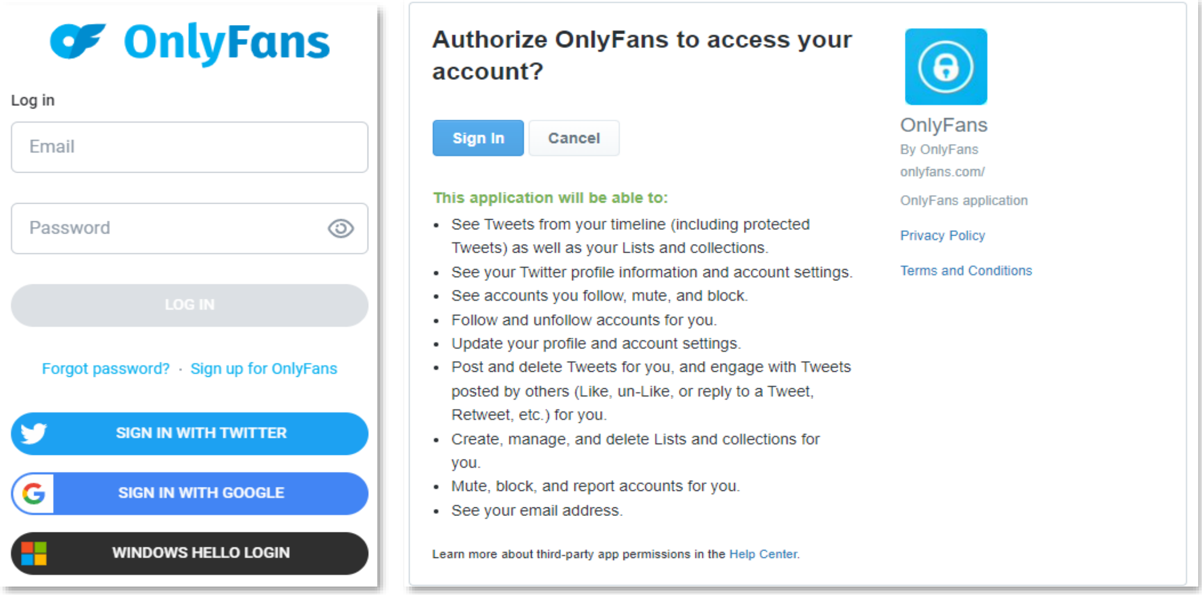
Account-based assurance or cross-account authentication allows a user to share attributes such as their age by logging into an existing account, such as their Facebook or Google account, when accessing an age-restricted site. Once logged in, the provider of the existing account shares the user's information through an application programming interface (API).

Level of assurance

The level of assurance is dependent on the method used to assess age for the original account and how the age-restricted site uses that data. Assurance levels can be compromised. For example, in 2021, researchers were able to sign up for an Only Fans account (which requires users to be 18) by logging in with Google using an account with a self-declared age of 13.[403]

Feasibility and effectiveness

Cross-authentication is common practice with users logging into many apps and services using third-party logins (for example, Facebook, Google, Apple, Amazon and WeChat).



Authorize OnlyFans to access your account?

This application will be able to:

- See Tweets from your timeline (including protected Tweets) as well as your Lists and collections.
- See your Twitter profile information and account settings.
- See accounts you follow, mute, and block.
- Follow and unfollow accounts for you.
- Update your profile and account settings.
- Post and delete Tweets for you, and engage with Tweets posted by others (Like, un-Like, or reply to a Tweet, Retweet, etc.) for you.
- Create, manage, and delete Lists and collections for you.
- Mute, block, and report accounts for you.
- See your email address.

Learn more about third-party app permissions in the Help Center.

Figure 8 Using other accounts to sign into OnlyFans

[403] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021.

Accessibility, barriers to inclusion and potential for bias

Account-based assurance requires a pre-existing account (usually with a major service). Sole use of this method risks excluding those who cannot, or choose not to, use those services.

Requiring users to link accounts may affect the ability to craft and curate unique online identities in different forums.[404] Unlinked online identities can allow people to explore their identity and talk openly about issues such as their sexuality, without being 'outed' to their family, friends, or professional connections on other platforms.

Linking accounts to major service providers also risks limiting people's digital inclusion and rights to participate online if there is an error or issue with the central account and no fast and accessible way to resolve it. Stakeholders from the domestic adult industry told eSafety they often face challenges when large social media platforms apply their guidelines unevenly or change them without notice.[405]

Sensitivity of data

To provide age assurance, particularly for lower risk services, only the age attribute is required to be shared. However, in practice, account-based assurance can involve the sharing and consolidation of large amounts of data about a user. For example, when using Twitter to log into OnlyFans (above), the user's tweets, account information, and email address are shared, along with the ability to post or delete tweets and interact with others on the service.

Research from Ofcom in the UK revealed most families were aware of cross-service authentication and some had occasionally used it across social media platforms.[406] Children reported they could remember seeing this option but did not understand how it worked and what impact it had on their information. Parents generally indicated they did not want to use account-based assurance because they did not want their information to be used to build detailed profiles of themselves across platforms.

Overall assessment of account-based assurance

The use of account-based assurance may involve privacy risks for individuals where personal information is shared across platforms and is used to build more detailed individual profiles that are used for targeted advertising, among other things. Individuals would need to be informed about the information being shared between platforms if account-based assurance was utilised. Even with this disclosure, it is difficult to assess the extent of privacy risks and

[404] M Ingram, '*Why ending anonymity would not make social media better*', Columbia Journalism Review, 4 February 2021, available at: https://www.cjr.org/the_media_today/why-ending-anonymity-would-not-make-social-media-better.php; E van der Nagel and J Frith, *'Anonymity, pseudonymity, and the agency of online identity: Examining the social practices of r/Gonewild', First Monday,* 2015, 20(3), DOI: 10.5210/fm.v20i3.5615

[405] See Appendix 5.

[406] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

whether they are proportionate to the goal of establishing one's age to access a service. In addition, cross-account authentication as a method of age assurance is only effective if the underlying account applies robust age assurance measures.

Platforms and services which offer account-based assurance (non-exhaustive list)

- Facebook
- Onlyfans

AI profiling or inference models

Profiling involves making predictions or determinations about a user (including their age) based on data collected as a user interacts with a service. For example, Facebook looks at the age in users' public birthday messages to flag if a user might be underage.[407]

Many sources of data can be used to make predictions, with varying rates of accuracy and invasiveness. This can include information inferred through a user's interactions – how long they spend on a page, the age of their connections/followers on a site, and their stated interests.[408] Other data includes mobile data usage or finger swiping patterns.

Level of assurance

The level of assurance provided by this technology depends on dataset quality. Several social media services have internal mechanisms for gauging the age of their users but auditable reports on their accuracy are not publicly available. According to Ofcom's research, both parents and children in the UK doubt the reliability and accuracy of behavioural profiling.[409]

Feasibility and effectiveness

This technology is currently in use and is further detailed in chapter 11. Several academic papers have proposed approaches for estimating social media users' ages by analysing their posts. A 2018 paper examined a range of algorithms for identifying genders and age groups of social media accounts by analysing the contents of their posts.[410] Researchers considered factors including 'sociolinguistics, grammar, characters and words.' A 2022 paper evaluated a method that automatically identified the age of users based on self-reports in their tweets.[411] The natural language processing algorithm the researchers developed analysed more than 1.2 billion tweets posted by more than 245,000 users and was able to predict ages for 54% of them.[412]

Another profiling tactic involves determining a person's age by analysing mobile phone data and usage patterns. A 2019 paper proposed a method for predicting mobile device users' gender and age based on their behaviour, services they use, and contract information.[413] The model achieved

[407] Meta, '*How Facebook knows an app user is old enough*', 2021, available at: https://about.fb.com/news/2021/07/age-verification.

[408] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021.

[409] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

[410] J Cheng et al., *'Age and gender profiling of social media accounts', Proceedings of the Pacific Asia Conference on Information Systems,* 2017, available at: https://web.archive.org/web/20220804124912id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1194&context=pacis2017.

[411] A Klein, A Magge and G Gonzalez-Hernandez, *'ReportAGE: Automatically extracting the exact age of Twitter users based on self-reports in tweets*', *PloS ONE*, 2022, 17(1):e0262087, DOI: 10.1371/journal.pone.0262087.

[412] A Klein, A Magge and G Gonzalez-Hernandez, *'ReportAGE: Automatically extracting the exact age of Twitter users based on self-reports in tweets*', 2022.

[413] I Al-Zuabi, A Jafar and K Aljoumaa, *'Predicting customer's gender and age depending on mobile phone data',* Journal of Big Data, 2019, 6(18), DOI: 10.1186/s40537-019-0180-9.

85.6% accuracy in predicting users' gender and 65.5% accuracy in predicting their age. A separate study by Zhejiang University in China and the University of South Carolina claimed to distinguish between young children and adults based on their mobile phone screen swipes and tapping[414] although the findings were limited.

Accessibility, barriers to inclusion and potential for bias

As with all assessments based on AI, the technology will be influenced by the data set on which it is trained. Biases in that dataset can be replicated in applying the technology.

Sensitivity of data

Ofcom's research revealed this was the least popular choice in the UK, with few parents supporting its use.[415] It was seen as being potentially privacy invasive, and participants were unclear about how much data would need to be processed and collected to estimate a user's age. Concerns were also raised about data being used inappropriately or for purposes other than age verification. Several eSafety Youth Council members also felt this method was invasive. Informed consent processes must be used when implementing this technology to make sure user understand and agree to profiling and inference measures to support their online safety.

An individual's interactions with a pornography website may reveal or infer sensitive information, such as sexual orientation or practices. A detailed profile of a user can be built where their interactions with a service are combined with other information. This has great value to organisations beyond age assurance and could attract risks of secondary use and disclosure that may be privacy invasive or harmful to the individual.

Overall assessment of AI profiling

This technology relies on the user interacting with the service before it can profile their age and could be effective as a secondary layer to self-declaration on some platforms and services (depending on the purpose or their use and risk of accessing online pornography).

Individuals must be clearly and fully informed about how their information is collected, used and disclosed. Without oversight, it also risks large data collection and surveillance of users which can also be used for commercial purposes. This is an important tool for identifying children who have bypassed age assurance measures used at the sign up stage.

[414] R Metz, '*A phone that says 'no' to little kid fingers*', MIT Technology Review, 2018, available at: https://www.technologyreview.com/2018/02/09/241284/a-phone-that-says-no-to-little-kid-fingers/.

[415] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

Platforms and services which use AI profiling and inference models (non-exhaustive list)

- Facebook
- Instagram

Biometric age and capacity assessment

Biometric methods analyse a person's characteristics, such as their face or voice, to estimate their age. Capacity assessments analyse a person's aptitude, such as reading comprehension, to estimate their age.

Facial analysis - Machine learning models are used to estimate a person's age based on their facial proportions and characteristics. There are several facial age assessment products available in the market, each at various stages of maturity. 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.

Voice print age assessment - Machine learning technology typically asks a user to talk about a particular topic, answer a question, or read out a paragraph from the device screen. It can assess many voice characteristics including pitch, cadence, and delivery. Enex TestLab concluded this method is not currently as mature as facial age assessment, but its accuracy is improving. Some age assurance product vendors use it in conjunction with facial analysis.

Capacity assessment - This method estimates a user's age by assessing their aptitude or capacity. The technology seeks to assess qualities such as a user's sentence structure, language sophistication, and concept comprehension to estimate their age. In written form, the technology can analyse how users type and their keystroke patterns. This method is not as mature as facial estimation and involves substantial risk of accessibility challenges and bias.

Level of assurance

These techniques are used to estimate, rather than verify, age. Accordingly, there will always be a rate of error. Enex TestLab found facial analysis technology is currently the most mature and promising option within this category. Enex TestLab also pointed out voice analysis and capacity testing tend to be limited by the fact that a person's ability to read, speak or write does not always correlate to their biological age.

Feasibility and effectiveness

Facial analysis for age is increasingly being taken up by large online services. It appears voice and capacity analysis are less common practices.

The integration of device-based biometrics such as Apple's Face ID and Touch ID into browsers such as Safari has also created new opportunities for low-friction ways for users to verify their identity to log in to websites.[416] Some stakeholders who participated in our consultations felt

[416] Apple Support, '*Use Face ID on your iPhone or iPad Pr'o*, Apple, available at: https://support.apple.com/en-au/HT208109

there was great potential for this technology to support age verification efforts. Others held concerns about using security features for safety purposes.

Capacity testing can be effective for very young ages. A Chinese app 'Baby bus' (for children aged 2-8), requires users to match traditional Chinese characters with numbers to turn off parental control settings.[417] This is an easy task for many adults, but challenging for very young children.

It is unclear how financially feasible this technology would be for smaller providers of age-restricted goods or services. It is possible that with time, competitive and affordable methods will become available for a range of businesses and contexts, including through a charging framework which distributes costs across multiple industries. Affordability concerns demonstrate the need for any mandated regime to provide service providers flexibility in compliance, considering their individual circumstances and risk factors.

Accessibility, barriers to inclusion and potential for bias

The potential for bias within each of these options was frequently raised as a concern by stakeholders during consultations. It was also identified as a concern by eSafety's Youth Council. Both parents and children in the UK expressed doubts about accuracy, noting the appearance of teenagers can vary widely given differences in the age of puberty and development.[418]

The ICO's age assurance opinion warns 'systems based on biometrics such as hand or facial structure may perform poorly for people of non-white ethnicity, or for those with medical conditions or disabilities that affect physical appearance'.[419] Capacity testing can create barriers for people with intellectual disability or brain injury and voice assessments may be affected by accents, low language fluency or disability.

Apps and websites which use biometric data need to be digitally inclusive so all users can access and use digital technologies in their day-to-day lives.[420] Digital inclusion can be impacted by factors such as the affordability of devices and an internet connection, how easy it is to access an internet connection, and the presence of digital skills to navigate digital environments.[421] The Australian Digital Inclusion Index in 2021 shows that 1 in 4 Australians were

[417] F Liu, '*Designing for kids: Cognitive considerations*', Nielsen Norman Group, 2018, available at: https://www.nngroup.com/articles/kids-cognition/.

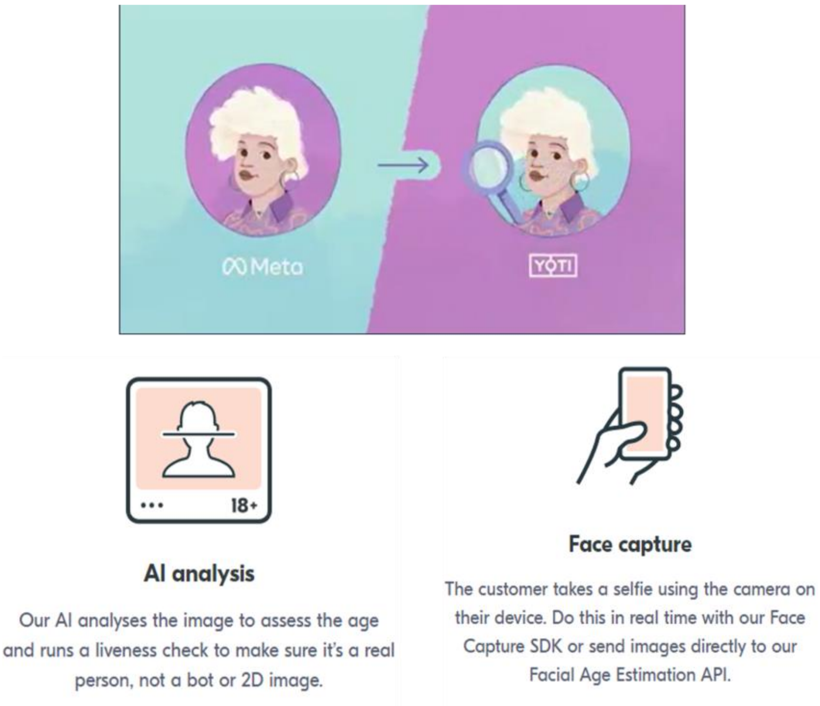
[418] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

[419] UK Information Commissioner's Office (ICO), '*Information Commissioner's opinion: Age assurance for the Children's Code*', 2021, available at: https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf.

[420] Be Connected, '*What is Digital Inclusion?',* available at: https://www.beconnectednetwork.org.au/news-events/what-digital-inclusion.

[421] Good Things Foundation Australia, '*The Digital Divide',* available at: https://www.goodthingsfoundation.org.au/the-digital-divide/

digitally excluded.[422] Those who are digitally excluded are more likely to be on low incomes or unemployed, people with a disability, older Australians, or those living in regional areas.[423]



AI analysis

Our AI analyses the image to assess the age and runs a liveness check to make sure it's a real person, not a bot or 2D image.

Face capture

The customer takes a selfie using the camera on their device. Do this in real time with our Face Capture SDK or send images directly to our Facial Age Estimation API.

Figure 9 Yoti age estimation service for Meta

Sensitivity of data

Biometric templates and biometric information used for the purpose of automated verification or identification is 'sensitive information' under the *Privacy Act 1988* (Cth). In eSafety's public perceptions research, 40% of respondents said they would be comfortable with face, fingerprint, or voice scanning for age estimation purposes; 37% said they were not comfortable; 20% didn't know; and the remainder did not respond.[424]

Assessment by French privacy regulator French data privacy regulator, Commission Nationale de l'Informatique et des Libertés (CNIL) advised that age estimates based on biometric facial analysis should preferably be performed locally on a user's device to reduce the risk of data leakage. CNIL also found this method should not be used without an independently verified framework of operating, reliability and performance standards. This is due to the intrusive and sensitive nature of the data and the margin of error inherent in statistical evaluation.[425]

[422] J Thomas, J Barraket, S Parkinson, C Wilson, I Holcombe-James, J Kennedy, K Mannell and A Brydon, '*Australian Digital Inclusion Index: 2021*', RMIT, Swinburne University of Technology and Telstra, 2021, DOI: 10.25916/phgw-b725, available at: https://researchbank.swinburne.edu.au/file/ab6218ee-55f3-4d84-9174-76ca9ec877be/1/2021-thomas-measuring_australias_digital.pdf

[423] Thomas et al., *Australian Digital Inclusion Index: 2021.*

[424] eSafety Commissioner, '*Public perceptions of age verification for limiting access to pornography*', available at: https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography.

[425] Commission Nationale de l'Informatique et des Libertés (CNIL), '*Online age verification: balancing privacy and the protection of minors*', 2022, available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

As 'sensitive information', heightened privacy protections apply to the collection, use or disclosure of biometric information and templates. This is in recognition of the fact biometric information and templates are unique and inalienable to the individual, and therefore warrant particular protection. Sensitive information may only be collected with consent unless an exception applies, and more stringent requirements apply to its use or disclosure. It is important to note that facial recognition and facial estimation vary in the identifying information they process and although data is processed it does not need to be retained after enabling verification.

In the Attorney-General's Department Report on the Review of the Privacy Act[426], it is proposed that:

- The collection of biometric information for use in facial recognition technology should be prescribed as an exception to the small business exemption in the short term, while other steps are taken to remove the exemption for small businesses (proposal 6.2(a)).[427]
- All entities bound by the Australian Privacy Principles (APPs) be required to complete a Privacy Impact Assessment prior to undertaking a 'high privacy risk activity', which could include the use of biometric templates or biometric information for the purpose of verification or identification when collected in publicly accessible spaces. This should be done as part of a broader consideration by government of the regulation of biometric technologies (proposal 13.1 and 13.2)
- Collection, use and disclosure of personal information must be 'fair and reasonable in the circumstances' (proposal 12.1.).

Increased protections for the collection, use and disclosure of biometric information and templates may support trust and confidence in the use of these technologies for age assurance.

The risks related to the use of biometric information and templates for facial recognition technology depend on each particular application, and the way in which the technology is deployed.[428] The privacy risks may be more significant and intrusive where biometric information is used to identify an individual out of a database of many individuals (one-to-many matching) as opposed to confirming whether a photograph matches the photograph of the same person

[426] Attorney-General's Department (AGD), '*Privacy Act Review report*', 2023, available at: https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[427] Currently, small businesses with an annual turnover of $3 million or less are exempt from coverage under the Privacy Act except in limited circumstances. This proposal would mean that small businesses who collect biometric information for use in facial recognition technology would need to comply with the Privacy Act in relation to those activities.

[428] See discussion on facial recognition technology and biometrics in chapter 13 of Attorney-General's Department (AGD), '*Privacy Act Review report*', 2023, available at: https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

held by that entity (one-to-one). In recognition of information sensitivity, some of these technologies perform their analysis on a user's device and delete the input once the analysis has been undertaken- so as not to retain any data. It is important to reiterate that biometric 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. eSafety does not believe that the use of facial recognition technology is necessary or applicable to determining one's age to permit access to online pornography.

Overall assessment of biometric age and capacity assessment

The use of biometrics must be supported by stringent standards, effective legislation and protections for users. However, biometric tools offer a privacy preserving, age assurance solution in that a person's identity is not linked to their facial analysis and these tools can be designed to delete input once an age assessment has been made. This strongly reduces risks associated with data collection, storage and misuse. The primary challenges with these technologies that must be addressed as potential ethic bias and scalable costs. Facial analysis emerged from Enex TestLab's review as a potentially viable and privacy-preserving way to estimate age, however the technology is still evolving and maturing.

Platforms and services which use biometric age and capacity assessment (non-exhaustive list)

- Yoti
- Instagram
- Yubo
- TikTok

Hard identifiers

Hard identifiers can be used to verify a person's age either through viewing the physical version of a document, uploading a copy for its details to be extracted and validated using optical character recognition and verification against an existing database. Where using a photo ID, users may also be required to share a real-time photo of themselves so it can be compared with the photo on the ID document.

Hard identifiers are a very accurate age assurance method, particularly when paired with liveness checks. Hard identifiers are often used for offline age-restricted goods and services. However, the accessible personal information is above what is necessary to determine if a user meets the applicable age range (for example, 18+). The collection of personal data can have significant consequences such as identity theft (if data is misused or leaked).

People may be more likely to use hard identifiers through pre-existing trusted systems and services that already hold that data – or through trusted systems and services such as digital wallets which only share limited information. However, as hard identifiers are strongly tied to identity, this may limit the circumstances where people feel comfortable using them. It is important to consider user choice and offer a variety of tools and methods to make sure there is an appropriate age assurance method for all users.

Level of assurance

Government-issued identity documents such as birth certificates, passports, and driver's licenses provide a high level of assurance to verify a person's age, due to strict proof-of-identity requirements.

A service can use a record date or proxy as proof, or they can employ a third-party identity verification company such as Equifax or the Australia's Government's Document Verification System to confirm the validity of the document.

Proof or proxy

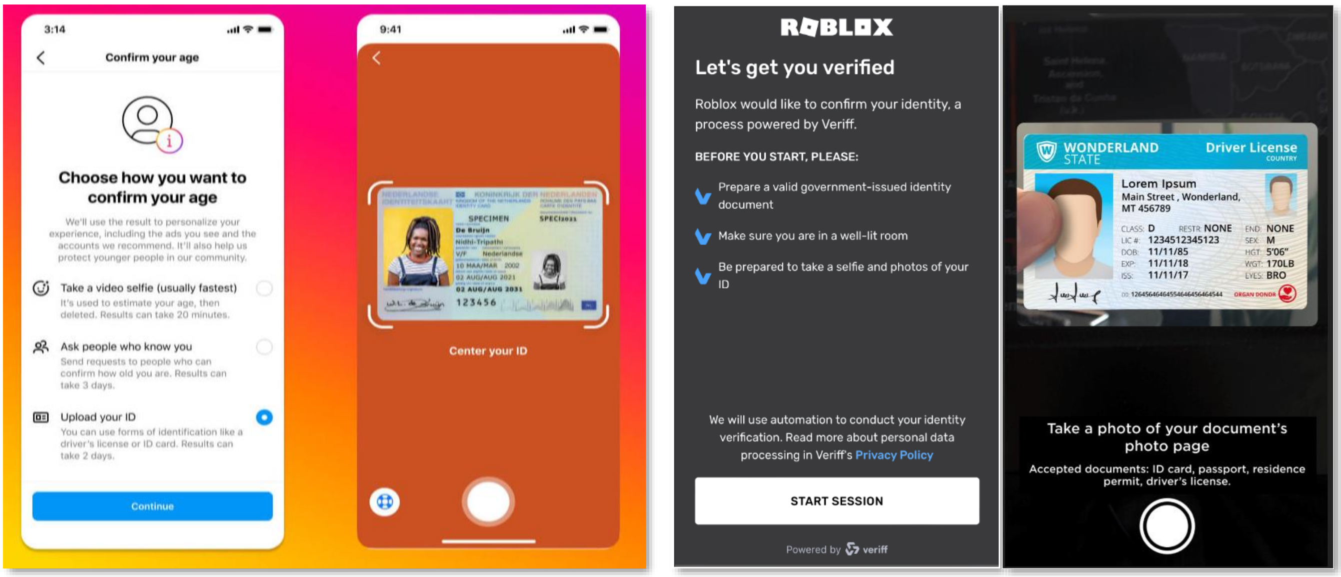
The relevant age attribute can be within the record itself – such as passports or driver's licenses – or the record can act as a proxy. For example, in jurisdictions where a person must be over 18 to have a credit card or sign a mobile telco contract, those records can be used as evidence a user is over a certain age.

Feasibility and effectiveness

Hard identifiers with photos such as passports and driver's licenses are commonly used when accessing age-restricted goods and services in-person such as when purchasing alcohol or accessing licensed premises. Enex TestLab's view was that the most effective way to reliably determine a person's age is to use trusted documents such as birth certificates, passports, and other photo ID.

In offline situations, services can confirm the purchaser is using their own identity documents by matching their face to their photo ID, although this becomes challenging if a user is accessing services online or over the phone.

Hard identifiers have been implemented online for variety of services. Roblox, Google, Meta, and Discord all provide means for users to verify their age using government identity documents. YouTube allows users to verify their age using credit card details. Stakeholders from the domestic adult industry reported they also commonly use credit card details (as their content is behind paywalls) as a proxy method to verify age of users who access their sites.



Confirm your age

Choose how you want to confirm your age

We'll use the result to personalize your experience, including the ads you see and the accounts we recommend. It'll also help us protect younger people in our community.

○ Take a video selfie (usually fastest)
It's used to estimate your age, then deleted. Results can take 20 minutes.

○ Ask people who know you
Send requests to people who can confirm how old you are. Results can take 3 days.

● Upload your ID
You can use forms of identification like a driver's license or ID card. Results can take 2 days.

Continue

Center your ID

Let's get you verified

Roblox would like to confirm your identity, a process powered by Veriff.

BEFORE YOU START, PLEASE:

- Prepare a valid government-issued identity document
- Make sure you are in a well-lit room
- Be prepared to take a selfie and photos of your ID

We will use automation to conduct your identity verification. Read more about personal data processing in Veriff's Privacy Policy

START SESSION

Take a photo of your document's photo page

Accepted documents: ID card, passport, residence permit, driver's license.

Figure 10 Examples of age confirmation through identity documents

However, measures based on hard identifiers can be circumvented if a user has access to another adult users' documents. To mitigate this, some services implement a liveness test or live detection test and require a photo or video of the user at the time the verification request is made. This is an effective barrier, but also requires the processing of biometric data. However, although processed, the data does not need to be retained after enabling verification.

> '...IDs can be forged or altered, so relying on them as the sole means of verifying someone's age can be unreliable and IDs can be stolen or lost, and using them to

> verify age could potentially expose sensitive personal information to identity thieves' – eSafety Youth Council member

Accessibility, barriers to inclusion and potential for bias

According to data collected by the Australian Passport Office in 2019-20, only 57% of Australians own a passport.[429] Similarly, driver's licenses and birth records are not universally accessible. Requiring the upload and sharing of hard identifiers can also be challenging for people who are digitally excluded, such as people who do not have easy access to a mobile phone camera or other means to scan and upload documents.

Both consultation participants and members of eSafety's Youth Council noted that access to, and use of, government ID can be difficult for certain communities, including trans and gender diverse people, First Nations people, victim-survivors of family and domestic violence, and people who have lost documents in natural disasters. Some Australian banks have recently started providing identity verification as a service to retailers.[430] In Australia, children aged 14 and over can open bank accounts.

> 'Confirmation from phone providers or banks definitely bring down some of the access issues as older teens tend to have either one of those' – eSafety Youth Council member

The ICO's opinion on age assurance noted the risk of excluding or indirectly discriminating against people who do not have required documents. The ICO suggested organisations take a holistic approach to hard identifiers.[431] Similarly, AUSTRAC provides guidance on flexible application of Know Your Customer (KYC) procedures for Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) purposes. This can be applied in low-risk scenarios where people may not be able to produce the required documents.[432] Vouching, as an alternative, is discussed below.

Sensitivity of data

Government-issued ID often includes a photo, full name, date of birth, address, and other details, including government-related identifiers. Examples of government-related identifiers

[429] Department of Foreign Affairs and Trade (DFAT), *2019-20 passport facts*, Australian Passport Office, available at: https://www.passports.gov.au/2019-20-passport-facts.

[430] J Eyers, 'Banks ready to launch new digital identity checking service', *Australian Financial Review*, 31 August 2022, available at: https://www.afr.com/companies/financial-services/banks-ready-to-launch-a-new-digital-identity-checking-service-20220830-p5bdzn.

[431] UK Information Commissioner's Office (ICO), *Information Commissioner's opinion: Age assurance for the Children's Code*, 2021, available at: https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf.

[432] AUSTRAC (Australian Transaction Reports and Analysis Centre), *Assisting customers who don't have standard forms of identification*, available at: https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification.

include Medicare numbers, Centrelink Reference numbers, driver's license numbers issued by state and territory authorities, and Australian passport numbers.[433] International IDs may include more information. For example, US driver's licenses include information about the holder's sex/gender and physical characteristics.

Government-related identifiers are sometimes regulated by specific laws that restrict the way in which they can be collected, used and disclosed by other entities. For example, tax file numbers and individual healthcare identifiers are subject to specific legislation. In addition, APP 9 in the Privacy Act sets out restrictions in relation to government-related identifiers as that term is defined in the Privacy Act.

Government-issued IDs contain valuable information that can be used for identity theft, such as a passport or license number. As a result, collection and storage of these details presents privacy and data security risks. If multiple entities are required to collect and store government-issued identifiers, this can exacerbate these privacy and data security risks. The use of interoperable age verification tokens assists in addressing these risks. They are discussed in more detail below.

Consultation stakeholders expressed concerns about using government-issued ID to access online pornography. However, in our public perceptions research, 62% of respondents said they would be comfortable providing a driver's license and 54% said they would be comfortable scanning a photo ID to enable an age check.[434] Ofcom-commissioned research in the UK found both parents and children overwhelmingly preferred hard identifiers above all other measures for websites featuring pornography and gambling, though some felt it was 'too much' on social media sites.[435] While they felt this would provide an effective way to verify age, most families also expressed concerns over the sharing of this information and the potential for data breaches or identity fraud. The storage of other information, such as credit card details, is also of concern.

Third party providers

In consultations, stakeholders raised some of the benefits in using third-party age assurance providers, including users being more comfortable providing their information to these providers rather than a social media platform, pornography site, or other online service.

[433] Office of the Australian Information Commissioner, '*Read the Australian Privacy Principle's,* 2019, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles.
[434] eSafety Commissioner, '*Public perceptions of age verification for limiting access to pornograph'y*, available at: https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography.
[435] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

Stakeholders noted that large online services may stand to benefit commercially from the collection and on-selling of user data, whereas third-party providers are incentivised to minimise data collection to reduce privacy and security risks.

Conversely, stakeholders also highlighted that some users may have greater trust in the underlying site or service than a lesser-known third-party age assurance provider. Stakeholders noted that trust can be built through awareness raising, accreditation and certification schemes, transparency, oversight, and redress mechanisms.

Comments from eSafety Youth Council members

'I think the fact that the actual identification is in another service besides the social media makes me, and hopefully others, feel safer' – eSafety Youth Council member

'My initial thoughts were that I would be a lot more comfortable with using ID such as passports or driver's licenses. However, I believe I would only be confident in giving my ID only to government websites and apps. I have used ID for WWCC, myGOV and other government-related websites and felt relatively confident with it. Though, if it's for some social media platform like Instagram or Facebook, I won't feel confident as I feel like providing my ID would be giving more information than just my age' – eSafety Youth Council member

'Even though I've verified my identity on Facebook and Google with my debit card previously, I'm scared of man-in-the-middle attacks or services storing my financial details' – eSafety Youth Council member

Overall assessment of hard identifiers for age verification

Hard identifiers are a very high assurance method for identifying a user's age, particularly when paired with liveness checks. However, the personal information on many hard identifiers is above what is necessary to determine a person is over a certain age. Additional personal data can be collected, which can cause significant consequences, including the risk of identity theft if that data is misused or leaked. Enex TestLab's view was that the most effective way to reliably determine a person's age is to use trusted documents such as birth certificates, passports and other photo ID.

Although this method provides the highest assurance, there are significant privacy and data security concerns that must be addressed through policies, standards, and regulation if this method were used in any mandatory regime. This includes the risk of breaches if data is collected and stored, as well as challenges regulating the data use if processed overseas.

Preferably, only the use and sharing of a user's age attribute would be permitted for the purpose of accessing age-restricted goods and services. In addition, any use of hard identifiers should align with the Australia's *Trusted Digital Identity Framework (TDIF)*. A whole-of-government approach to verifiable credentials should also be considered.

Platforms and services which use hard identifiers (non-exhaustive list)

- Roblox
- Google
- Instagram
- Discord

Vouching

Vouching, or attestation, is a method used to confirm a person's age where a trusted entity with an existing relationship to the person vouches for that person.[436]

This can include:

- where an account holder (usually a parent or carer) confirms the age of another user (their child)
- where an institution or community organisation confirms the age of a user.

Offline, vouching is commonly used in situations where a person does not have government-issued ID, such as a passport or birth certificate. For example, referee statements are used for Anti-Money Laundering and Counter-Terrorism Financing purposes.[437]

Some stakeholders suggested telecommunications providers and ISPs which are already required to collect personal information about their users may be well placed to support vouching. Others flagged that these entities are more likely to collect information of parents than children, as those under 18 generally require an adult to sign them up for a post-paid account.

Level of assurance

The level of assurance may vary depending on the circumstances and who is vouching. Where the vouch is provided by a trusted institution, with a high likelihood of having accurate knowledge of a person's age and identity, this can provide a high level of assurance. A vouch can be combined with other evidence for a higher level of confidence. UK Government guidance suggests a vouch can be checked for strength, validity, and to make sure the claimed identity has existed over time, which means it is less likely to have been recently made up.[438]

Feasibility and effectiveness

Meta has tested social vouching for verifying a user's age on Instagram.[439] Users can ask mutual followers to confirm their age. The vouching users are required to meet safeguards set by Instagram, although these safeguards are not publicly listed. In October 2022, this method was removed as an option while improvements were made. As at March 2023, it has not returned as

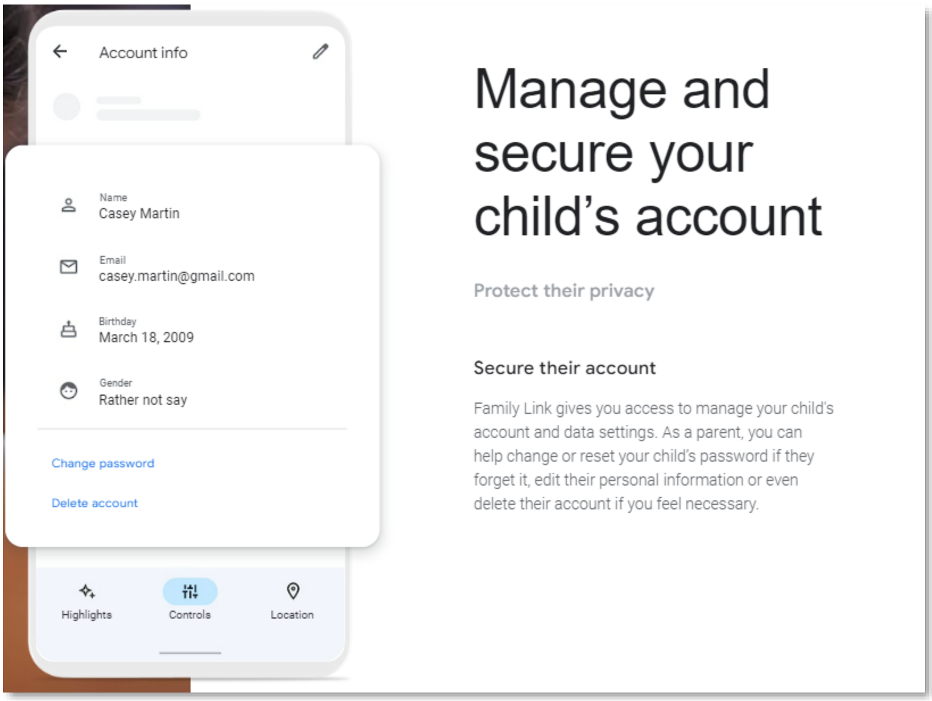
[436] Example of vouching as an accepted practice in the UK: UK Government Digital Service, '*How to accept a vouch as evidence of someone's identity*', UK Government, 2020, available at: https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-a-vouch-as-evidence-of-someones-identity.

[437] AUSTRAC (Australian Transaction Reports and Analysis Centre), '*Assisting customers who don't have standard forms of identification*', available at: https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification.

[438] UK Government Digital Service, '*How to accept a vouch as evidence of someone's identity*'.

[439] Meta, '*Introducing new ways to verify age on Instagram"*, 2022, available at: https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram.

an option. Ofcom-commissioned research found parents in the UK liked the concept of parent or guardian vouching for a user's age as it gave them control and flexibility and created opportunities to communicate with children about what they are doing online.[440] However, they had questions about how this would work in practice and expressed reservations about using this measure in the context of access to pornography, preferring more stringent age assurance technologies in those circumstances.[441]



Account info

Name
Casey Martin

Email
casey.martin@gmail.com

Birthday
March 18, 2009

Gender
Rather not say

Manage and secure your child's account

Protect their privacy

Secure their account

Family Link gives you access to manage your child's account and data settings. As a parent, you can help change or reset your child's password if they forget it, edit their personal information or even delete their account if you feel necessary.

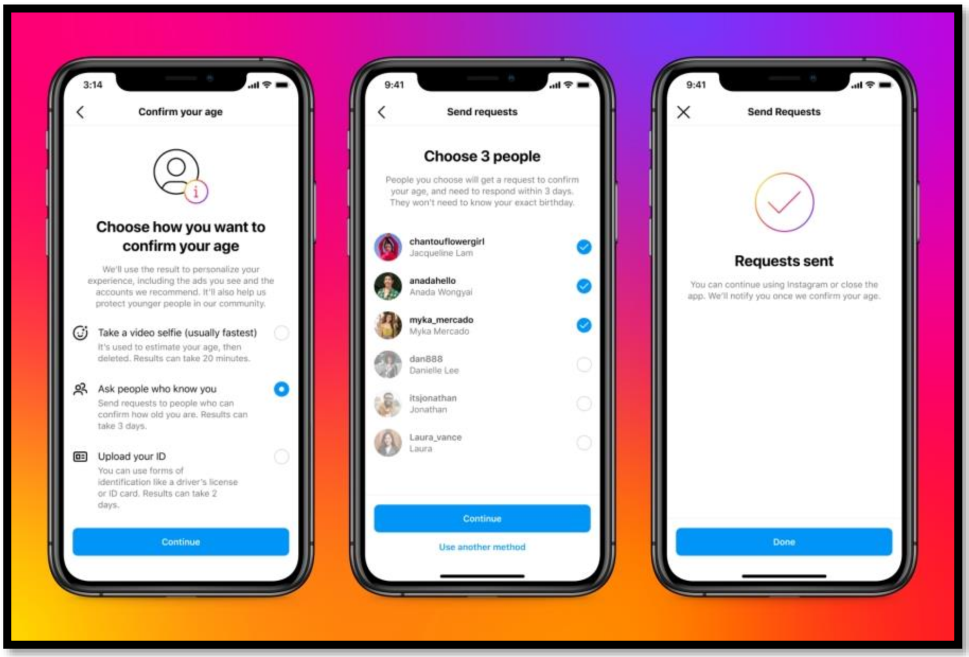
Figure 11 Google guidance on how to use Google Family Link

Accessibility, barriers to inclusion and potential for bias

This option is meant to overcome barriers, such as lack of access to ID. As highlighted by the Age Verification Providers Association, vouching by professionals such as teachers can be one of the most inclusive methods of age assurance, as it does not require users to have any specific documents or records.[442] However, when determining which entities can engage in vouching, it is important to note that relationships with institutions such as banks and universities are not universal. Similarly, it is unlikely that trusted institutions or professionals would offer vouching services to access online pornography.

[440] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.
[441] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.
[442] Age Verification Providers Association (AVPA), '*How do you check age online?*', available at: https://avpassociation.com/avmethods/.

Regarding parental vouching, not all children have an involved and supportive parent or other adult who can demonstrate legal guardianship. Where there is an involved parent, children in the UK expressed concern they may be excluded from some activities their peers were taking part in due to different rules among different parents.[443]



Choose how you want to confirm your age

We'll use the result to personalize your experience, including the ads you see and the accounts we recommend. It'll also help us protect younger people in our community.

○ Take a video selfie (usually fastest)
It's used to estimate your age, then deleted. Results can take 20 minutes.

● Ask people who know you
Send requests to people who can confirm how old you are. Results can take 3 days.

○ Upload your ID
You can use forms of identification like a driver's license or ID card. Results can take 2 days.

Choose 3 people

People you choose will get a request to confirm your age, and need to respond within 3 days. They won't need to know your exact birthday.

chantouflowergirl	Jacqueline Lam	✓
anadahello	Anada Wongyai	✓
myka_mercado	Myka Mercado	✓
dan888	Danielle Lee	○
itsjonathan	Jonathan	○
Laura_vance	Laura	○

Requests sent

You can continue using Instagram or close the app. We'll notify you once we confirm your age.

Figure 12 Meta's use of vouching on Instagram

Open Identity Exchange (OIX)

The Open Identity Exchange (OIX), formed in 2010, is a non-profit organisation whose objective is to address the increasing challenges of building trust in online identity. OIX has proposed a Digital Vouch with Photo option for 'ID-challenged' people. This includes:

- those who live in a jurisdiction where there is no comprehensive central government record for all.
- those who lack government-issued ID such as passports or driver's licenses, which may be required to enrol in Digital ID in their jurisdiction.
- those who are not captured within relevant databases, such as credit databases, which are relied upon as part of the proofing process in their jurisdiction.

[443] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

OIX proposes this option could be used for online age verification purposes and to produce a digital photo verification 'token'. Tokens are discussed in more detail later in this chapter.

Sensitivity of data

Data sensitivity in vouching depends on what is required. If a simple attestation is provided to confirm a person is above or below a certain age, there is relatively low sensitivity. However, the individual's association or relationship with the vouching entity may reveal sensitive information. If the vouching entity is a parent, proof of that relationship would be required.

Child accounts may also raise issues about children's privacy online, particularly as they get older. As with account-based assurance, linking accounts (in this case, a parent/carer and a child account) can provide services (such as social media platforms) with detailed profiling information about both individuals.

Overall assessment of vouching

Depending on the context and purpose for which age is being confirmed, vouching and associated methods can be an important alternative option to consider for those who may lack access to documents and whose age may not be accurately assessed using other options. In terms of privacy, vouches are best applied where the verifying party cannot see the purpose of the vouch as there is a high risk of stigmatising users and impacting on their digital participation.

UK parents interviewed by Ofcom preferred the control and flexibility of confirming their children's ages, and often used similar measures for gaming and social media accounts already (for children aged 18 and under).[444]

Platforms and services which use vouching (non-exhaustive list)

- Google Family Link, when parents set up an account for their child, and enter that child's age.

[444] Revealing Reality, '*Families' attitudes towards age assurance*', Ofcom and ICO (Information Commissioner's Office), 2022.

Methods of sharing a verified age, age attribute, or age range

Once a person's age has been assessed using any of the above or other methods, their age (or age attribute) needs to be shared with the age-restricted online service they are trying to access. The ability to re-use one's age assessment can reduce some of the friction, frustrations, and pricing challenges for businesses and consumers.

Devices

Some stakeholders saw an opportunity to provide age-appropriate online experiences by embedding the user's age within their device's operating system. These stakeholders believed device and operating system options would be the most scalable, simplest and comprehensive for parents as they reduce the need to configure different settings and permissions for different sites. Similarly, these options support the principle of being privacy preserving, as they remove the need for data collection across multiple services. Stakeholders believed people have higher levels of trust in device manufacturers than in other online services to keep their data safe, noting consumers are accustomed to providing personal information to companies to purchase and set up a device.

Stakeholders pointed out that parents often have more control over their children's devices than their online accounts and have an incentive to input their child's correct age if the device asks for it. The age, age range (13-17) or age attribute (18+) could then be transmitted to relevant age-restricted areas of the digital ecosystem, with controls in place to prevent children from adjusting the age once confirmed on the device. It was noted that in some instances children may set up their own devices, particularly where parents or carers have lower levels of digital literacy.

There are also instances where devices are shared by family members. While some stakeholders felt this could be easily overcome by enabling different profiles for each device user – with PINs or biometrics employed to recognise users and unlock the correct account – others did not believe security features should be applied in this context. Some stakeholders also raised concerns that mandating the use of these measures for age verification could serve to further consolidate the market power of the leading device companies.

Age tokens

Enex TestLab and several stakeholders noted that a tokenised approach to age assurance holds great potential to reduce friction and enhance user privacy.

Once a person's age has been verified or estimated, data can be converted into a re-usable electronic 'token.' Rather than providing a user's specific age, these tokens can be limited to confirming that a user does or does not meet a minimum age requirement. This allows the service to confirm age requirements are met without viewing or collecting personal information. It also reduces friction for users by minimising how frequently they must confirm their age.

Tokens can be designed to expire after a pre-determined period, such as after an online session, to prevent them from being reused later by someone else.[445] Other authentication measures, such as on-device facial recognition or passwords, can also be activated when accessing one's age token, to prevent use by others.

Age tokens can be stored on a user's device within an app, digital wallet or saved using **cookies**. Some services are moving away from using browser cookies to identify users as they had already provided their age. AgeVerify, a UK provider of self-declaration age assurance, uses session storage instead.[446] Yoti allows users to create an 'age account' where they store their age tokens and re-use them on additional browsers and devices by logging into their account.[447]

Digital identity and wallets

A **digital identity** is a digital representation of a person which contains various attributes and credentials. Attributes can include a person's name, age, place of birth, citizenship and more. A credential is a record kept in electronic form by an identity service provider that contains authenticated identity information about an individual (for example, a driver's license) and is assigned a unique code by the service provider. Verified identities, attributes and relevant credentials can be stored in a digital wallet for re-use later. This report refers to digital identity as a concept and is not intended as a refence to Digital Identity under the Australian Government Digital Identity System.

A **digital wallet** is the app or software which allows users to store or share attributes of their digital identity. It offers users control over which attributes they share and for how long (users can revoke permissions). In practice, some services which accept digital identities can request

[445] A web session is a group of user interactions with a website that take place within a given time frame. Google analytics may expire a session using the time-based method which is either after 30 minutes of inactivity or after 24 hours. See Google, '*How a web session is defined in Universal Analytic*'s, Google Help Centre, available at: https://support.google.com/analytics/answer/2731565.

[446] AgeVerify, '*Big change – AgeVerify no longer uses cookie'*s, 2021, available at: https://ageverify.com/big-change-ageverify-no-longer-uses-cookies/.

[447] Yoti, '*Reusable age checks*', available at: https://developers.yoti.com/v8.0/age-verification/age-tokens.

more information than is necessary to confirm a user's age.[448] Decentralised or self-sovereign identity (SSI) systems are discussed in chapter 7 as a future development that may address some of the challenges associated with existing digital identity technology.

Multiple jurisdictions are exploring the use of digital wallets for purposes of verifying identity, age, and other attributes both within, and across, their borders. For example, the Council of the European Union has announced a goal of providing all EU citizens a strong set of universal digital identity credentials that will be recognised anywhere in the EU.[449] These credentials will be accessible from a digital wallet and available to anyone from their mobile device. The EU Digital Identity Wallet Consortium is conducting a large-scale pilot for the wallet's ecosystem in early 2023 focusing on the use of digital identity in the context of travel (providing passenger information), buying goods and services, and for trusted business-to-business interactions.[450] The European Commission has also committed to exploring how to use the EU Digital Identity Wallet for age assurance purposes. It will encourage and collaborate with Member States to issue digital IDs to children under 18, which it believes could lead to a private and secure EU-wide recognised proof of age attribute.[451]

Europe is not alone utilising digital identity for purposes of age assurance. The US state of Louisiana has recently legislated the use of 'LA Wallet' as an acceptable way for pornography sites to meet the new requirement for verifying that users are 18+.[452] Commentators have raised privacy concerns due to a lack of clarity around whether the state of Louisiana would be able to discern that a person had used LA Wallet to access pornography. There is also confusion as to whether pornography sites access an individual's age attribute or all the personal details on the user's digitised ID.[453] These concerns could potentially be addressed by establishing double-blind attribute exchanges, like those being tested in France and through the euCONSENT project.

[448] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021.

[449] Council of the EU, '*European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europ'*e, 2022, available at: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/.

[450] EU Digital Identity Wallet Consortium, '*Press Release: EWC has been selected by the European Commission to participate in EU Digital Identity Wallet Large Scale Pilots*', 2022, available at: https://eudiwalletconsortium.org/2022/12/14/14th-dec-2022/.

[451] European Commission, '*New European strategy for a better Internet for kids*', 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826.

[452] Louisiana State Legislature, *House Bill No. 142*, 2022, available at: https://legis.la.gov/legis/ViewDocument.aspx?d=1289498.

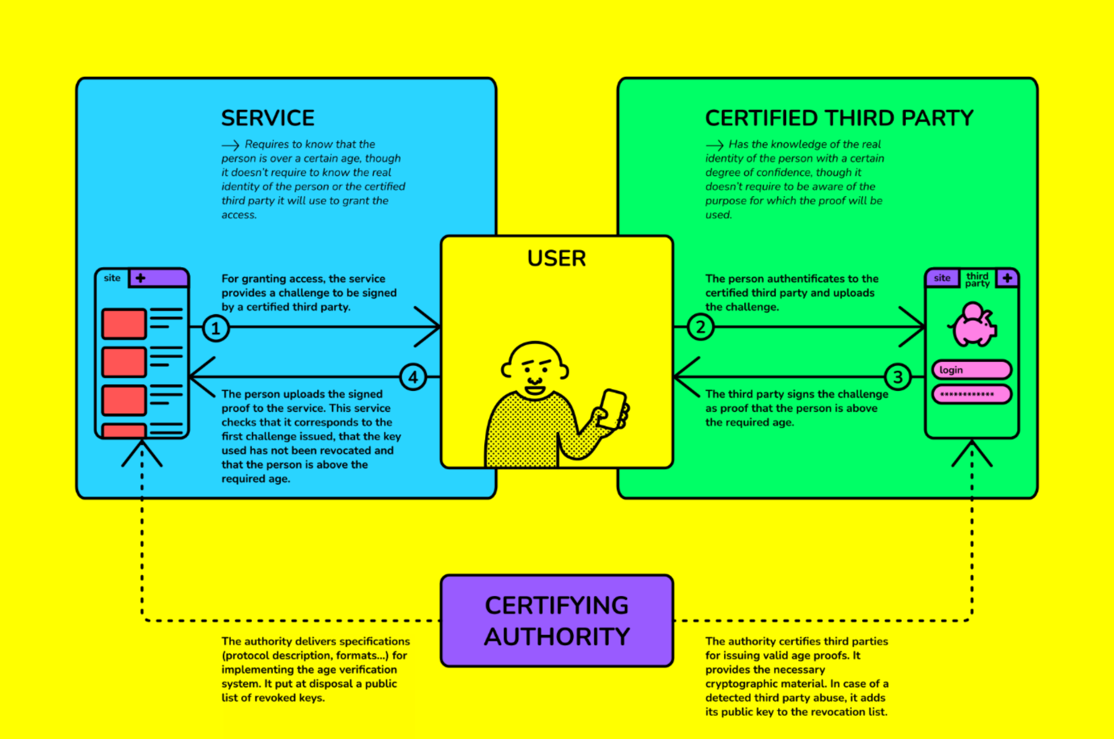
[453] P Hutchinson, *'Age verification law for adult websites comes with privacy, technical concerns',* Louisiana Illuminator, 11 January 2023, available at: https://lailluminator.com/2023/01/11/age-verification-law-for-adult-websites-comes-with-privacy-technical-concerns/.

Double-blind methods and exchanges

In eSafety's consultations, stakeholders raised the benefits of zero-knowledge proof methods or **double-blind systems** as examples of privacy-preserving approaches to age assurance.

A **zero-knowledge proof** method is based on a process in cryptology, allowing individuals to prove their age without having to reveal any other information. A third-party exchange acts like a switchboard, transferring information (with a person's consent) between sites or platforms requiring age confirmation and services which estimate or verify age. The exchange only transfers information which the person consents to be shared. This may be a birthdate, an age or simply confirmation a person is over 18.

The Laboratoire d'Innovation Numérique de la CNIL (Digital Innovation Laboratory of the CNIL LINC)[454] conducts experimental projects and develops prototype tools, services and concepts around data for CNIL.[455] LINC is a partnership with cryptography researchers and the PEREeN. In June 2022, LINC released an open-source demonstration of the zero-knowledge proof method which can be found at on its website. [456]



SERVICE

→ *Requires to know that the person is over a certain age, though it doesn't require to know the real identity of the person or the certified third party it will use to grant the access.*

1 For granting access, the service provides a challenge to be signed by a certified third party.

4 The person uploads the signed proof to the service. This service checks that it corresponds to the first challenge issued, that the key used has not been revocated and that the person is above the required age.

CERTIFIED THIRD PARTY

→ *Has the knowledge of the real identity of the person with a certain degree of confidence, though it doesn't require to be aware of the purpose for which the proof will be used.*

2 The person authentificates to the certified third party and uploads the challenge.

3 The third party signs the challenge as proof that the person is above the required age.

CERTIFYING AUTHORITY

The authority delivers specifications (protocol description, formats...) for implementing the age verification system. It put at disposal a public list of revoked keys.

The authority certifies third parties for issuing valid age proofs. It provides the necessary cryptographic material. In case of a detected third party abuse, it adds its public key to the revocation list.

Figure 13 LINC demonstration of Implementing the zero-knowledge proof method

[454] LINC (Laboratoire d'Innovation Numérique de la CNIL), '*About LINC*', 2016, available at: https://linc.cnil.fr/propos-de-linc.

[455] CNIL, Commission Nationale de l'Informatique et des Libertés, is France's National Data Protection Commission.

[456] J Gorin, M Biéri and C Brocas, '*Demonstration of a privacy-preserving age verification process*', LINC, 2022, available at: https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process.

Double blind method: example user journey

1. A user visits an age-restricted website and is prompted to verify their age.
2. The user is redirected to a third-party exchange which hosts a range of companies that provide age assurance. The user opts for a biometrics-based age estimation service from a company they recognise.
3. The age assurance service assesses the user as 30 years old and sends the exchange the verified age attribute.
4. The exchange then provides the age-restricted website with a confirmation that the user is 18+.
5. The age-restricted website only receives the age confirmation, while the age assurance service does not have access to where the attribute has been used.
6. After the information is transferred, it is then deleted by the exchange.

Assessment of current market products

Enex TestLab assessed a limited number of technologies available in the market, offered by third-party providers for use on a range of online services. Their assessment was complemented by eSafety's landscape scanning and desktop research about the providers.

Biometrics

Enex TestLab's assessment of biometric estimation tools included Privately and Yoti.[457] Their evaluation was limited by several factors, including time constraints, the extent of information made available by companies, and the lack of a comprehensive, age-verified data set against which accuracy could be tested.

To overcome the latter challenge, Enex TestLab enlisted 14 test subjects between the ages of 3 and 21. These test subjects performed simple tests in their own homes using their own devices and integrated cameras under the best possible lighting conditions. The test subjects ran the same biometric analyses five times, under the same environmental conditions, to determine reliability.

While Enex TestLab statistically analysed the test data for the purposes of this report, the sample sizes were small and the methodologies were simple. The results obtained cannot be compared to larger-scale laboratory testing of these products.

Product 1 – Yoti's age estimation tool

Yoti is a UK-based digital identity company with offices in several countries, including Australia. It began in 2014 with a free, re-usable digital ID app and now provides a range of verification services spanning identity and age verification, eSigning, and authentication.[458]

Yoti's age verification service offers users six ways to prove their age:

- Age estimation based on facial analysis (the solution tested)
- Reusable digital ID through the Yoti app
- One-time verification through a scanned ID document
- Credit card check
- Mobile provider check
- Database check

[457] Enex reached out to Ageify but did not receive information to enable testing in time for this report.
[458] Yoti, '*Age verification*', available at: https://www.yoti.com/business/age-verification/.

Yoti's age estimation approach uses a 'neural network' – a computing technique which is designed to reflect the behaviour of the human brain to allow computer programs to recognise patterns.[459] Yoti's age estimation demo has been trained to estimate human age using a process of 'machine learning'. This involved the program being fed millions of diverse facial images with accompanying ages to help it 'learn' how to match an age estimation to a users' photo. [460]

Yoti generally requires internet connectivity and for data to be sent to their servers to work. However, it has recently developed a model which can operate offline or directly on a device. Yoti suggested this model is only 8.4% less accurate than their online model.[461]

How testing was carried out

Enex TestLab used the web version of Yoti World's 'Estimate Your Age' demo[462] to test the accuracy of the program against 14 users, aged between 3 and 21 years old. Each user made five attempts at using Yoti's age estimation demo, which requires users to scan their face into the web page using a mobile phone camera or web camera.

Results

- 64% of tests classified subjects in the correct age bracket.
- 53% of results averaged over multiple tests classified the correct age bracket.
- On average, the midpoint of the estimated age range differed from the true age by 21%.
- The true age was, on average, only 6% outside the estimated age bracket.
- The assumed age estimation (mid-point of returned range) differed on average by 1.6±0.5 years from the actual age with a standard deviation of 2.8 years.
- If only the magnitude of the error is considered, without considering if the estimate is over or under the actual age, the average error is 2.6±0.5 years.
- In some cases, the estimated age of a subject varied markedly over five tests; with one seven-year-old assigned ages in the range 6 to 14.

Enex TestLab concluded that the accuracy of Yoti's tool was 'quite good', exceeding the performance of some other tools tested, although they found Yoti had a slight tendency to overestimate the age of younger children in Enex TestLab's tests. As noted above, the small

[459] IBM, '*What are Neural Networks?*', available at: https://www.ibm.com/topics/neural-networks.
[460] Yoti, '*Yoti age estimation white paper*', 2022, available at: https://www.yoti.com/blog/yoti-age-estimation-white-paper.
[461] Yoti, *Yoti age estimation white paper*, 2022.
[462] Yoti, '*Age estimation*', available at: https://yoti.world/yoti-age-estimation-demo/.

sample size of Enex's testing means these results are not directly comparable to the results produced by researchers with a significant sample size.

Yoti's publicly available research claims their True Positive Rate (TPR) for 13-17-year-olds being correctly estimated as under 23 is 99.93%.[463] This is close to the 96% TPR calculated in Enex's testing. However, while Yoti claims the TPR for 6-11-year-olds being correctly estimated as under 13 is 98.91%, Enex's testing achieved only 60% TPR for this age range. The small testing sample and lack of diversity of testers may account for this differential.

Yoti - response to independent testing

In response to the results of Enex TestLab, Yoti has sought to clarify that Enex TestLab's assessment was based on their public demonstration tool. Yoti stated that the public demo does not include liveness detection, return an uncertainty value, or use the current version of their estimation algorithm. As a result, Yoti states the assessment results do not accurately reflect the experiences of Yoti's commercial clients. Yoti also submitted that the sample size was insufficient to draw conclusions.

The report from Enex TestLab is at **Appendix 8** and Yoti's full response is at **Appendix 9**.

Feasibility

Social networking app Yubo has used Yoti age verification tools for third-party age verification since 2019.[464] In May 2022, Yubo fully integrated Yoti's age estimation software into their systems.[465]

In June 2022, Meta began using Yoti's facial analysis tool to allow US Instagram users to verify their age.[466] During this pilot, age verifications tools (including Yoti), reportedly stopped 96% of teenagers from attempting to edit their date of birth to make them over 18.[467]

In October 2022 this trial was expanded to countries including Brazil and India before being rolled out to Facebook Dating in December 2022.[468] Instagram users in Australia, Canada, Europe, Japan Mexico and South Korea were able to begin using Yoti's facial estimation tools from March 2023.

[463] Yoti, '*Yoti Facial age estimation white paper*', 2023, available at: https://www.yoti.com/blog/yoti-age-estimation-white-paper.

[464] Yubo, '*Using AI for good on Yubo',* available at: https://www.yubo.live/newsroom/using-ai-for-good-on-yubo.

[465] S Perez, *'Gen Z social app Yubo rolls out age 'estimating' technology to better identify minors using its service',* TechCrunch, 26 May 2022, available at: https://techcrunch.com/2022/05/25/gen-z-social-app-yubo-rolls-out-age-estimating-technology-to-better-identify-minors-using-its-service/.

[466] Meta, '*Introducing new ways to verify age on Instagram*', 2022, available at: https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram.

[467] Meta, '*Bringing age verification to Facebook Dating',* Facebook, 2022, available at: https://about.fb.com/news/2022/12/facebook-dating-age-verification/.

[468] Meta, *Bringing age verification to Facebook Dating,* Facebook, 2022.

Yoti was also used in a 2022 UK supermarket trial to allow shoppers to verify their ages at checkout for age-restricted purchases, such as alcohol.[469] Reports suggest the trial was successful, with most shoppers supportive of the technology and welcoming the opportunity to use it again. Yoti was also included in the euCONSENT pilot and has been used by OnlyFans.

Sensitivity of data

Yoti collects a scan of a user's face using a camera. Yoti also states it deletes all biometric data as soon as the age check is conducted. Yoti claims that if you put the same face into the model several times, it would not be able to identify it as a face it has seen before and would provide a new and different estimation each time.[470] Accordingly, Enex TestLab did not deem Yoti's age estimation software to be overly sensitive.

Yoti says it does not involve the processing of special category data under the European Union's General Data Protection Regulation (GDPR) as it does not allow for the unique identification or authentication of a natural person.[471]

Security and technical integrity/certification, accreditation or auditing/trustworthiness

Yoti is certified to meet the requirements of ISO/IEC 27001, the global standard for information security management.[472] It was also externally audited over a six-month period and received SOC 2 Type II certification[473] for its compliance with five trust principles – security, availability, processing integrity, confidentiality, and privacy – against the American Institute of Certified Public Accountants' Trust Services Criteria.[474]

Yoti's website notes the architecture of its security systems has been reviewed by Cigital (Synposus) and it regularly undergoes penetration testing to look for potential vulnerabilities in its security operations.[475]

Yoti is accredited under:

- BSI PAS 1296:2018 and the Age Check Certification Scheme (discussed in chapter 9)[476]

[469] F Hersey, *'Success of age estimation, digital ID trials in UK lead to pressure for changes to the law'*, Biometric Update.com, 2023, available at: https://www.biometricupdate.com/202301/success-of-age-estimation-digital-id-trials-in-uk-lead-to-pressure-for-changes-to-the-law.

[470] Yoti, *Yoti age estimation white paper*, 2022.

[471] Yoti, *Yoti age estimation white paper*, 2022.

[472] Yoti, '*DAS certification*', 2022, available at: https://www.yoti.com/wp-content/uploads/DAS-32111239_0_I-Yoti-Ltd-2022-2024-Rev-004.pdf.

[473] Yoti, '*Our approach to security and privacy*', 2019, available at: https://www.yoti.com/blog/our-approach-to-security-and-privacy/.

[474] IT Governance, *SOC 2 audits,* available at: https://www.itgovernance.co.uk/soc-reporting.

[475] Yoti, '*Our approach to security and privacy*', 2019, available at: https://www.yoti.com/blog/our-approach-to-security-and-privacy/.

[476] Age Check Certification Scheme, '*Yoti Ltd – Age check certification*', available at: https://www.accscheme.com/registry/yoti-ltd.

- the German Association for Voluntary Self-Regulation of Digital Media
- the German Kommission fur Jugendmedienschutz (KJM) accreditation (discussed in chapter 10).[477]

Accessibility, barriers to inclusion and potential for bias

There are no significant barriers to accessibility or inclusion identified in Enex TestLab's assessment of Yoti. However, it should be noted that as the *Estimate Your Age* tool requires users to align their face with an on-screen frame, this tool may not be suitable for people with vision impairment.

Research literature has revealed age accuracy biases in facial age estimation when comparing females to males and for some ethnic groups.[478] Yoti has acknowledged their data set used for training the Estimate Your Age tool skews towards males, particularly those with light skin tones.[479] This has led to a 22% difference between the highest and lowest skin tone accuracy across 6-29-year-old females.[480]

Yoti has also acknowledged that conditions which affect facial appearance can make a minor impact on the way the tool works but suggests it does not materially affect age estimations.

Transparency and accountability in relation to decision-making, and availability of appeals processes

While Enex TestLab noted Yoti does not provide users with insight into the decision-making process leading to the age range given, we note that overall Yoti offers a considerable level of transparency. It makes a variety of information on the validity of its testing available to the public, including the impact of factors such as skin tone.[481]

Yoti has undergone in-depth testing by an accreditation lab as part of the Age Check Certification Scheme, which certified the accuracy of the company's age estimation technologies.[482]A scan of publicly available information did not find information about an appeals process. Some online services which have incorporated Yoti's age estimation tools have

[477] Yoti, *Age verification.*
[478] K Kärkkäinen and J Joo, *'FairFace: Face attribute dataset for balanced race, gender, and age for bias measurement and mitigation',* Proceedings of the IEEE Winter Conference on Applications of Computer Vision (WACV), 2021, 1547, DOI: 10.48550/arXiv.1908.04913, available at: https://openaccess.thecvf.com/content/WACV2021/html/Karkkainen_FairFace_Face_Attribute_Dataset_for_Balanced_Race_Gender_and_Age_WACV_2021_paper.html.
[479] Yoti, *Yoti age estimation white paper*, 2022.
[480] Yoti, *Yoti age estimation white paper*, 2022.
[481] Yoti, *Yoti age estimation white paper*, 2022.
[482] Age Check Certification Scheme, *Yoti Ltd – Age check certification.*

provided users with alternative age assurance options where users believe Yoti has incorrectly estimated their age.[483]

Governance and risk management processes

Yoti is governed by a Board and a Guardian Council – an independent ethics board comprising experts from relevant fields such as human rights and data privacy.[484] Meeting minutes from the Guardian Council are available on Yoti's website, dating back to 2016.

Yoti has publicly supported initiatives such as the 5Rights framework and Responsible 100 to make sure its product is ethical.[485] A scan of publicly available information did not find information about risk management processes.

Flexibility to account for different business models

Yoti provides a software developer kit (SDK) and an API for clients which allows businesses to adapt the product for their needs.[486] Yoti also provides guidance on user experience to help clients when designing their web or mobile integration.[487] Yoti's pricing structure is tiered to provide charities with discounted or free access to Yoti's products.[488]

A prospective client of Yoti who was interviewed by Enex TestLab said the cost of implementing Yoti's technology for purposes of age gating an app can be about $1 per app downloaded by each user. One interviewee said this cost could not be sustained by smaller companies with a modest number of paid subscribers. Yoti has included further information on their pricing structure in their response to the independent assessment at **Appendix 9**.

Product 2 – Privately's age estimation tool

Privately, a Swiss-based company, was launched in 2014 as an offshoot of security firm Kudelski.[489]

Privately's age estimation product uses 'deep learning' - a computing technique which uses real-life examples to learn complex mathematical models to detect age.[490] Privately uses multiple forms of biometrics in its age estimation, including images of a user's face, their voice

[483] Epic Games, '*Parental consent for epic accounts*,' available at: https://www.epicgames.com/site/en-US/parental-consent.
[484] Yoti, '*Ethical framework*', available at: https://www.yoti.com/ethical-framework/.
[485] Yoti, '*Ethical framework*'.
[486] Yoti, '*Quick start integration guid'e,* available at: https://developers.yoti.com/age-estimation/quick-start.
[487] Yoti, '*User experience*', Yoti website, available at: https://developers.yoti.com/age-estimation/user-experience.
[488] Yoti, '*Third sector commitment',* available at: https://www.yoti.com/third-sector/
[489] Privately, '*Privately*', available at: https://www.privately.eu/; Natasha Lomas, '*Oyoty is a chatbot designed to teach kids to be safe online*', 2016, available at: https://techcrunch.com/2016/10/19/oyoty-is-a-chatbot-designed-to-teach-kids-to-be-safe-online/.
[490] ICO, '*Privately- Age appropriate design code engagement report executive summary*', 2021, available at: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019196/privately-aadc-exec-summary-202112.pdf.

pattern, and writing.[491] There are currently two types of solutions offered by Privately: SDK and on-browser. The age estimation models used by Privately are performed on the end-user's device. This privacy-preserving method means biometric data never leaves the user's device.[492]

How testing was carried out

Testing was undertaken by 14 users aged three to 21 using Privately's online demonstration website. This site captures video to test the face, image and voice analysis of a user.[493] In practice, users need to download the Privately app to their browser or device.

In Enex TestLab's testing, four age ranges were provided for both face and voice: 0–13, 13–17, 18–24 and 25+. The 0–13 category for face was not tested in Enex's demonstration. These ranges fit with the age limits of 13 for most social media and 18 as a generally accepted age of adulthood.

Results

Face

- 34% of tests classified test subjects in the correct age bracket.
- 29% of results averaged over multiple tests classified the correct age bracket.
- On average, the actual age was nearly three years outside the estimated age bracket.
- Over five tests per person, the results were often consistent with each other.

Voice

- 44% of tests classified test subjects in the correct age bracket.
- 31% of results averaged over multiple tests classified in the correct age bracket.
- On average, the actual age was about four years outside the estimated age bracket.
- Over five tests per person, the results were often highly variable – for example, a single 12-year-old was classed as 13–17, 18–24 and 25+ in successive tests.
- These results exclude the case of one seven-year-old child who remained silent during the voice test and was classified as an adult.

[491] Privately, '*Multimodal Age Estimation*', available at: https://www.privately.eu/age-estimation/.
[492] ICO, *Privately- Age appropriate design code engagement report executive summary*, 2021.
[493] Privately, '*Age estimation demo',* available at: https://showroom.privately.swiss/.

The age ranges generated by Enex TestLab's testing differs from the age ranges detailed by Privately. While Enex TestLab was only able to see four age ranges, other reports claim Privately models are trained to estimate seven different age ranges (0-7, 8-12, 13-17, 18- 25, 26-34, 35-49, and 50+).[494] Privately's ACCS 1:2020 accreditation by the Age Check Certification Scheme states the May 2022 version of its age estimation system can accurately estimate the age of a nominal 18-year-old as being under the age of 25 with 95.69% reliability. The mean absolute error, mean predicted age, and upper and absolute tolerances were within permitted parameters set out in ACCS 1:2020 Technical Requirements for Age Estimation Technologies.[495]

Enex TestLab's results showed voice analysis to be less accurate than the face analysis in the higher age ranges. Privately's tool accurately judged 0–13 for some younger children, but children as young as six were identified as adults by the voice analysis.

Feasibility

In February 2023, Privately announced it was working with behavioural biometrics company Nviso Japan to integrate age verification into digital kiosks for customers buying age-restricted products in Japan.[496] Privately's website also states its technology has been integrated into the recently launched Wup app,[497] which provides children with child-friendly information about media literacy.[498]

Enex TestLab did not report on any further real-world use cases supporting Privately's feasibility. It did note Privately requires users to download an app to carry out processing on their device, which may present barriers to implementation in some circumstances.

Sensitivity of data

As previously noted, some stakeholders strongly believe biometric data such as facial images and voice recordings are sensitive. However, Privately states that no biometric data leaves the user's device, which minimises the risk of sensitive data being breached.

[494] ICO, *Privately- Age appropriate design code engagement report executive summary*, 2021.
[495] Age Check Certification Scheme, '*Privately SA certification*', available at: https://www.accscheme.com/registry/privately-sa.
[496] A Macdonald, '*Nviso, Privately partner to integrate age verification solution into emotion-sensing Japanese retail kiosks*', Biometric Update.com website, 2023, available at: https://www.biometricupdate.com/202302/nviso-privately-partner-to-integrate-age-verification-solution-into-emotion-sensing-japanese-retail-kiosks.
[497] Privately, *Privately*.
[498] Pro Juventute, '*Knowledge and tips on how to use a mobile phone for children and parents for the first time*', available at: https://www.projuventute.ch/de/wup-app.

Security and technical integrity/certification, accreditation or auditing/trustworthiness

Privately is accredited under the Age Check Certification Scheme[499] and the German KJM accreditation (discussed in later chapters).[500] Privately states its age estimation SDK is compliant with the EU's GDPR and the US Children's Online Privacy Protection Act (COPPA).[501]

Accessibility, barriers to inclusion and potential for bias

As Privately offers a non-browser solution, it is generally accessible to users across operating systems. The Privately voice assessment requires users to be able to read and speak fluently, meaning it may pose challenges for younger users or those with limited literacy in the testing language. Additionally, the requirement for the user to place their face within the defined area on screen may make it inaccessible to people with vision impairment.

In developing the system, Privately has stated it has attempted to make sure each gender, skin tone, language, and other characteristics are fairly represented in both the training and test datasets, with similar proportions.[502] The scope of its Age Check Certification did not include testing for inherent bias.[503] As previously detailed, facial estimation technologies have known biases when comparing females to males and for some ethnic groups and skin tones.[504]

Transparency and accountability in relation to decision-making, and availability of appeals processes

Enex TestLab noted Privately does not provide users with insights or explanations about its decision-making. Privately does offer a publicly accessible online showroom with demos for different technologies.[505] A scan of publicly available information did not find information about appeals processes.

Governance and risk management processes

Privately has several advisors to the company, including a consultant child and adolescent psychiatrist who specialises in online safety, digital health, and technology.[506] A scan of publicly

[499] Age Check Certification Scheme, '*Privately SA certification*', available at: https://www.accscheme.com/registry/privately-sa.

[500] KJM (German Commission for Protection of Minors in the Media), '*KJM gives positive assessment to age verification system with biometric age verification*', 2022, available at: https://www.kjm-online.de/service/pressemitteilungen/meldung/kjm-bewertet-altersverifikationssystem-mit-biometrischer-alterskontrolle-positiv.

[501] Privately, *Multimodal Age Estimation*.

[502] ICO, *Privately- Age appropriate design code engagement report executive summary*, 2021.

[503] Age Check Certification Scheme, *Privately SA certification*.

[504] K Kärkkäinen and J Joo, 'FairFace: Face attribute dataset for balanced race, gender, and age for bias measurement and mitigation', 2021.

[505] Privately, *Age estimation demo.*

[506] Privately, *Privately*.

available information did not find information about broader governance or risk management processes.

Flexibility to account for different business models

Privately's age estimation technique can be integrated into apps, games, and devices, making it adaptable to multiple business models.[507] As Privately allows clients to use an SDK to adapt the tool to their needs, there is a degree of flexibility as to how it is rolled out. Enex TestLab was not able to determine the pricing structure of Privately's services.

Overall assessment of biometric age estimation

Enex TestLab noted these technologies are still evolving, and the global market remains relatively immature. Based on its testing, Enex TestLab concluded voice age estimation is less accurate than facial analysis. It noted this may have less to do with the maturity of the technology and more to do with the fact linguistic skills and fluency can be highly variable across people of all ages.

Enex TestLab was of the view facial age assessment is a 'front runner' technology, as 'it provides a reasonably accurate assessment but maintains user privacy because it doesn't permanently store unique personal data.' It found while facial age assessment is more reliable than voice age estimation, it also carries the potential for bias, including higher accuracy rates for males than females or lighter skinned people compared to those with darker skin. Closing this gap may take time and increased variety within AI training sets:

> 'For example, obtaining statistically valid results with facial age recognition would require many photos of people at various ages. It would also need a diverse training set to ensure it was relevant to the demographic of users who would rely on this technology. Given Australia's diverse population, it behoves us to ensure that any solution treats everyone without appreciable biases.'

[507] Privately, *Multimodal Age Estimation*.

Hard identifiers

Within the hard identifier category, Enex TestLab evaluated AgeChecked and Mastercard ID, producing a basic assessment of each tool. The assessment has been supplemented with additional desktop research conducted by eSafety.

Product 1 - AgeChecked identity verification

AgeChecked is an age and identity verification service provider that works primarily with online retailers selling age-restricted goods and services. The company was established in London in 2016.

The service provides customers with five main solutions[508]:

- Batch upload – allows customers to upload CVS files containing large amounts of data for age verification.
- Client API – takes place in the background as the customer enters their details at registration or checkout. AgeChecked verifies the customer is legally old enough to make the purchase.
- Consumer gateway – a pop-up verification appears on the customers' screen during their browsing experience.
- Secondary check - when using the Batch Upload or Client API channels, if AgeChecked is unable to verify the customer is over 18, a Secondary Check allows the customer to then choose from a range of additional verification options.
- ID scan – uses a mobile device to scan a customer's driver's license or other identity document and uploads it to AgeChecked's platform.

Feasibility

AgeChecked is used by eCommerce providers, such as Shopify and Woocommerce, to undertake age assurance for the purchase of alcohol online.[509] Current use cases include online gambling, the sale of knives, and broader retail.[510] It was also used in the euCONSENT pilot discussed below.

[508] AgeChecked, '*Age verification solutions for businesses*', available at: https://www.agechecked.com/solutions/.
[509] AgeChecked, '*WooCommerce plugin*', available at: https://www.agechecked.com/woocommerce-plugin/.
[510] AgeChecked, '*Testimonials*', available at: https://www.agechecked.com/testimonials/.

Sensitivity of data

AgeChecked states it does not hold any customer personal details. Instead, each successful age verification creates a 'unique anonymised token for that individual'.[511] The tokens are stored in AgeChecked's system against a hash of a users' email (in other words, the email address is turned into a string of code) for added security.

Security and technical integrity/certification, accreditation or auditing/trustworthiness

AgeChecked technology is based on the British Standard PAS 1296.[512] Additionally, AgeChecked states it is compliant with GDPR regulations and certified under ISO/IEC 27001 for information security management systems and their requirements.[513]

Accessibility and barriers to inclusion/potential for bias

AgeChecked relies on government issued ID to verify a user's age. This means there is a high likelihood that any potential customers without these documents would be excluded.

Transparency and accountability in relation to decision-making, and availability of appeals processes

An executive summary of AgeChecked's Age Check Certification Scheme audit report is available online.[514] A scan of publicly available information did not find information about the extent to which AgeChecked communicates its decision-making process to users. An interview with its CEO explains that once a customer has gone through the age check process, the retailer is able to see if they have passed, and if not, can provide alternate methods for verifying age.[515] There is no information available on appeals processes for the user.

Governance and risk management processes

There is limited public information on AgeChecked's governance and risk management processes. AgeChecked makes a public commitment to best practice in reducing underage access to age-restricted goods. It invites members of the public to contact either the company or the UK ICO with questions about how this is done or if they have concerns about their data privacy.[516]

[511] AgeChecked, *FAQs*, available at: https://www.agechecked.com/faq-2/.
[512] AgeChecked, *FAQs*.
[513] ISO, '*ISO/IEC 27001 requirements*', 2022, available at: https://www.iso.org/standard/27001.
[514] Age Check Certification Scheme, '*AgeChecked certification*', 2022, available at: https://www.accscheme.com/media/fgpghabb/agechecked-final-audit-report-2022.pdf.
[515] AgeChecked, '*Meet the company*', available at: https://channelx.world/2020/11/meet-the-company-agechecked/.
[516] AgeChecked, '*Public commitment*', available at: https://www.agechecked.com/public-commitment/.

Flexibility to account for different business models

Costs for AgeChecked services begin a €35/month for 100 checks, and there is a minimum contract length of 12 months.[517] AgeChecked notes it does not charge set up fees and does not charge for returning customers to a specific client's website.[518] AgeChecked highlights a variety of plugins and apps, as well as direct integrations, are available for businesses to integrate the AgeChecked platform into their website.[519]

Product 2 - Mastercard ID

Mastercard ID is a platform that allows users to upload hard identifier documentation to verify their identity and age at the same time. Users can then re-use this identity across multiple other platforms within Mastercard's digital wallet which supports Mastercard ID. The information collected may include government photo IDs and dates of birth.

Feasibility

Mastercard ID is designed to support a range of sectors, including financial services, retail, and government.[520] Since launching in Australia in 2019, Mastercard ID has partnered with Optus, Deakin University, Australia Post, Samsung, and Microsoft to provide identity verification services.[521]

Sensitivity of data

Mastercard ID asks users to upload a copy of their hard identifier documentation to verify their identity, including their age. Users then complete a face scan to set up their ID.[522] The product uses encryption and facial biometric authentication to make sure the user's information is secure on their mobile device.

Security and technical integrity/certification, accreditation or auditing/trustworthiness

Mastercard ID states all personal data and ID documents are stored with encryption. Since July 2022, Mastercard ID has been accredited in Australia under the Trusted Digital Identity Framework (TDIF) scheme. To become an accredited provider under the TDIF, providers must meet strict rules and standards for usability, accessibility, privacy protection, security, risk management, fraud control, and more.[523]

[517] AgeChecked, *FAQs.*
[518] AgeChecked, '*Meet the company*'.
[519] AgeChecked, '*Our trusted partners*', available at: https://www.agechecked.com/age-verification-channel-partners/.
[520] Mastercard, '*Innovation: Digital ID',* available at: https://www.mastercard.com.au/en-au/vision/who-we-are/innovations/digital-id.html.
[521] J Hendry, '*Mastercard's digital ID service accredited by government*', itnews, 2022, available at: https://www.itnews.com.au/news/mastercards-digital-id-service-accredited-by-government-583143.
[522] Optus, '*Introducing Mastercard digital ID*', available at: https://www.optus.com.au/customer-extras/mastercard-id.
[523] Australian Government, '*Trusted Digital Identity Framework*', Digital Identity System, available at: https://www.digitalidentity.gov.au/tdif.

Mastercard ID is accredited to identity proof level 1+. To access this service, users need to provide one acceptable identity documents such as a valid Australian driver's license or Australian passport. For some services, Mastercard ID requires users to provide biometric data such as scanning their face with a smart device.

Accessibility and barriers to inclusion/potential for bias

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.

Transparency and accountability in relation to decision-making, and availability of appeals processes

Mastercard's Global Privacy Notice states, depending on the user's country, they may have the right or choice to:[524]

- opt out of some collection or uses of their personal information
- access their personal information to rectify it, restrict or object to its processing or request its deletion, destruction or anonymisation
- receive their personal information to transmit it to another company
- withdraw any consent provided
- where applicable, lodge a complaint with the relevant supervisory authority or regulator.

Governance and risk management processes

Mastercard's statement on governance and sustainability states its work is *'driven by the belief that upholding the highest standards of ethics and responsibility is not optional – it is the only way to succeed in business in today's world'*. Its governance structures include a Management Committee and a Board of Directors with several Board Committees, including an Audit Committee and a Risk Committee.[525] Its governance guidelines, policies and reports and other corporate documents are available online.[526]

Flexibility to account for different business models

[524] Mastercard, '*Global privacy notice: Your rights and choice's*, 2023, available at: https://www.mastercard.com.au/en-au/vision/corp-responsibility/commitment-to-privacy/privacy.html#rights.
[525] Mastercard, '*Corporate governance*', available at: https://investor.mastercard.com/corporate-governance/default.aspx.
[526] Mastercard, *Corporate governance.*

Mastercard ID is compatible with any connected mobile device, making it accessible to a wide range of businesses.[527] There is no publicly available information regarding the cost of Mastercard ID.

Overall assessment of identity verification for the purpose of age verification

Digital age and identity verification based on hard identifiers is common practice 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.

The stakeholders eSafety consulted pointed to user hesitancy about providing ID in the specific context of accessing pornography, which was seen as highly sensitive and stigmatised. Some felt this hesitancy could potentially be minimised through a double-blind system, where the pornography service provider does not have visibility of the user's ID and the age assurance provider does not have visibility of the site or service being accessed. Stakeholders were also of the view that expanding age assurance processes to a wider range of age-restricted products and services beyond online pornography access – including gambling, alcohol sales and the like – could serve to normalise and ease discomfort about engaging in age assurance processes.

Both Enex TestLab and consultation stakeholders noted that reliance on hard identifiers creates barriers to inclusion. For example, smaller services that may lack resources to bolster their security or engage a third-party provider, as well as users who do not have access to relevant forms of ID. Stakeholders raised the importance of consumer choice across multiple options so users can select the best method to match their preferences and circumstances.

[527] Mastercard, '*Mastercard Identity Check'*, available at: https://www.mastercard.com.au/en-au/vision/who-we-are/innovations/digital-id.html

Case study: euCONSENT pilot

euConsent is a European Commission-funded project to develop an EU-wide network for completing online age verification and securing parental consent when younger children wish to share personal data.[528] Enabling consumer choice, reducing friction, protecting privacy, and normalising age assurance across a range of purposes were all considered in its development.[529] The objective of the network is to protect children from harm on the internet, particularly in relation to age-restricted goods, content and services while promoting their rights to the opportunities the internet offers. To date, euCONSENT has run two pilot projects.

First pilot[530]

The first pilot, conducted in September 2021, involved 63 adult participants from across Europe. The participants were asked to provide their age, complete three ‘missions’, and answer general questions about usability and applicability of the test system. The missions were to:

- Use an age verification provider to have their age checked for the first time, to buy alcohol from an online store.
- Use a previous age check to get access to the online store, without having to prove their age again.
- Access an online store by using a different age verification provider to the one directly supported by the store.

Trial results were primarily concerned with experimental design. It found improvements to the user interface were required to prevent user confusion. Technical data is not available in the first pilot report.

Second larger-scale pilot

The second pilot, conducted from February to March 2022, involved more than 1,700 people including children, parents and other adults.[531] Participants were selected from five countries in Europe with different relevant ages of digital consent under the GDPR: Belgium (13+), Cyprus (14+), Germany (16+), Greece (15+), and the UK (13+).

This pilot was a technical trial of how different providers of age checks and parental consent can share information with one another to enable access to a variety of age-restricted online

[528] euCONSENT, FAQ, available at: https://euconsent.eu/faq/.
[529] euCONSENT, *‘FAQ*’, available at: https://euconsent.eu/faq/.
[530] euCONSENT, ‘*Pilot execution report – Early pilot’*, 2021, available at: https://euconsent.eu/download/euconsent-pilot-execution-report-early-pilot/.
[531] euCONSENT, *‘Pilot execution report – First large scale euCONSENT pilot*’, 2022, available at: https://euconsent.eu/download/pilot-execution-report-first-large-scale-euconsent-pilot/.

experiences in a manner that protects users' privacy and is interoperable so that users do not have to complete the full age checking or parental consent process for every website they visit.

It was designed to offer consumers a range of service providers and age verification methods across different levels of assurance, including facial age estimation, or verification of a government-issued ID document or credit card. Participants selected a method of age verification on an initial site with that site's preferred provider, and then re-used that verification on subsequent sites which used different age verification partners. This occurred through an interoperable re-usable age token, which was saved on the user's browser. This meant no other information was exchanged between the providers (or the underlying dummy websites). A participant would only have to undergo an additional age check if the subsequent site required a stricter age check with a higher level of assurance.

Five dummy websites were created, each translated into four languages as applicable to the countries involved (English, French, German, and Greek). Sites included online stores for alcohol or knives, a dating site, a chat app, and a social media service. The alcohol and dating sites required users to be 18+ at a basic level of assurance. The knife store required users to be 18+ at a higher level of assurance. The social media service and the chat app required users to either establish they were at or above the age of digital consent in their country, or establish they had parental consent to use the service.

The trial used three age verification providers, all of which are members of the Age Verification Providers Association[532]:

- AgeChecked, which enables users to demonstrate their age through their driver's license, social media accounts, payment cards, address searches, or mobile network searches.[533]
- AGEify, which enables users to demonstrate their age through facial analysis, official document scanning, credit card, or human verification through a short video call.[534]
- Yoti, which enables users to demonstrate their age through facial age estimation, ID scans and selfies, or checks through databases, mobile providers, or credit cards.535

Where required, parental consent was obtained using JusProg, a German-based non-profit provider of parental control software, or Upcom, a company based in Turkey.[536]

While specific missions varied across three groups of participants, they included:

[532] Age Verification Providers Association (AVPA), '*AVPA members',* available at: https://avpassociation.com/members/.
[533] AgeChecked, '*Online age verification for businesses*', available at: https://www.agechecked.com/.
[534] Ageify, '*Ageify',* available at: https://age-ify.com/.
[535] Yoti, *Age verification.*
[536] I Corby, '*euCONSENT consortium awarded European Commission funding to create a child rights' centred cross-border system for online age verification and parental consent*', 2021, available at: https://euconsent.eu/euconsent-consortium-awarded-european-commission-funding-to-create-a-child-rights-centred-cross-border-system-for-online-age-verification-and-parental-consent/.

- Visiting an initial site and verifying their age using one of the methods provided.
- Visiting another site and re-using their previous age check, completing a further age check, and/or obtaining parental consent if they were under the age of digital consent.
- Visiting a third site and re-using their previous age check, undergoing an expedited parental consent process, or completing a further age check to a higher level of assurance for a more strictly regulated product or service.

Pilot take-aways

Most participants were able to complete the missions, though some challenges were reported.

Almost 81% of participants were able to complete at least two missions, and 63% managed to complete all three missions. Reported challenges included that estimated ages were different to actual ages and there were issues with document scanning, cameras, and resolution.

A small proportion of parents raised concerns about their children's privacy, while a majority (82% of one user group for the first mission) reported they were happy with the way age verification was performed on their child and felt the benefits outweighed the risks.

Interoperability between providers proved successful, but many participants did not re-use their age checks.

The performance of the system was rated favourably, with most participants reporting quick response times in all missions.

Pilot report authors concluded the interoperability between different age and parental consent providers worked reliably in nearly 100% of cases. However, among one of the user groups completing the second mission, 50% of participants ended up completing a further age check when they should have been able to re-use their first one. The report authors attribute this to participants either misunderstanding what they were meant to do, or potentially using a different device or browser than they had used in the first mission, which would prevent the re-use of their age token.

The report does not discuss some of the other potential challenges posed by relying on cookies, including users clearing their cookies; applying incognito or private browsing mode; sharing devices among family members of different ages who can then re-use a check that has been performed on an older relative; and restrictions under privacy legislation which require the consent of users and limit the length of time for which a cookie can persist.

Users appreciated having multiple age assurance options from which to choose.

The report authors raise a couple of reasons for this, one being that users are not ‘blocked’ if one method does not work for them, as they have alternatives.

Some of the accessibility challenges included itsme[537] not being available in all pilot countries; Yoti being limited to Android and iOS devices (not accessible via Microsoft Windows); and document scan not being an option for those without ID documents. Another reason is people’s perception of privacy varies. The same age assurance method can be regarded as very intrusive by some people, while others might feel comfortable with it.

Facial age estimation was a popular option.

For example, among one of the user groups in the first mission, 73% of children selected the facial estimation method, and in another group, 59% of children selected this option.

Pilot report authors attribute this to its ease of use, since it needs nothing beyond a selfie. Fifty per cent of children reported the age check was extremely easy to do, and more than 80% gave a positive answer. Those who gave a lower rating typically tried a method other than facial estimation.

Participants suggested future options could include integration with web banking or national registries, as well as scanning of student cards.

A substantial proportion of children were able to access sites meant for adults only.

Within one user group for a mission where children should have been denied access, 35% of children were granted access, and for another mission, 30% were granted access.

Pilot report authors attribute this to parents or other adults either completing the mission for the child or giving them the necessary information to do so (such as ID or credit cards), possibly due to a misunderstanding of the mission or because it was ‘only a survey’. However, given the pilot did not test for accuracy of the age verification methods, it cannot be determined whether some of these children gained access through erroneous results.

[537] ‘Itsme’ is a digital identity app for Belgian citizens, which was mistakenly required for some checks in other countries in the early stages of the pilot and subsequently resolved. See ING, *Itsme® for individuals*, available at: https://www.ing.be/en/individuals/daily-banking/all-about-itsme-for-home-bank.

Lessons for Australia

Enex TestLab identified several lessons to inform future decision-making in relation to the use of age verification and age assurance technologies.

The age assurance industry and its associated technologies are new and still evolving

Given time constraints and limited information available, it was difficult to fully compare products and provide a ranking across the criteria. However, Enex TestLab's assessment is that this is an immature market globally, with a small number of participants providing a diverse range of solutions to address the technical challenges of verifying age.

Very few of the available age assurance technologies appear to have undergone rigorous independent testing to determine their accuracy, error rate or potential for bias. Enex TestLab noted there are some exceptions to this. For example, Yoti has undergone in-depth testing by an accreditation lab.[538] The absence of publicly released testing among other providers does not necessarily indicate resistance; rather, it may stem from a shortage of relevant resources to conduct tests and the cost of obtaining tests.

Enex TestLab also offered the view that it would be beneficial to store tokens through digital wallets at the device-level rather than at the browser-level (which occurred in the euCONSENT pilot). eSafety recognises the importance of fostering innovation and growth in the safety tech sector and congratulates the euCONSENT team and its vendors for their cooperation in bringing an interoperable age assurance and parental consent system to life.

There are several positive features of the euCONSENT pilot that should be considered for the roadmap

One was the development of an internationally defined age token that can be linked to various age assurance technologies and online services, with identity information being purged once the person's age is verified and the token is created to protect privacy and prevent traceability back to an individual.

Another was the provision of multiple options for proof of age, which empowers users to choose a method in accordance with their privacy preferences and circumstances – including potential barriers such as lack of ID and issues with device compatibility.

Hard identifiers are more accurate in assessing age

While acknowledging accessibility issues, Enex TestLab emphasised that the most accurate way of creating reliable tokens is to use trusted documents such as birth certificates, passports, and other photo ID to verify a person's age. As facial analysis cannot provide precise age

[538] Age Check Certification Scheme, *Yoti Ltd – Age check certification*.

verification and may make significant errors in either direction, their view was its use should be provisional. Where the estimated age is close to an age cut-off, they suggested it may be part of a two-factor (or more) verification process.

A pilot in the Australian context is recommended

Enex TestLab suggested age assurance technologies should be trialled in the Australian context before being mandated.

They concluded that current published international standards are not comprehensive and mainly involve high level principles which may, by themselves, be insufficient to address domestic requirements. These standards are detailed in chapter 9.

Enex TestLab stated that any standards to be applied in the Australian context would need to be aligned with existing frameworks such as the Digital Transformation Agency's *Trusted Digital Identity Framework* for digital identity services and the Department of Social Services' *National Consumer Protection framework for online wagering*.

Based on the results of the euCONSENT trials in Europe, they recommended that any such trials should:

- Include a broad range of sites (such as alcohol sales, dating apps or gambling platforms) to avoid stigmatising an individual category such as pornography, and determine the appropriate level of assurance for each use case. Australian age assurance developments in online wagering and online alcohol sales are discussed in the chapter 9.
- Have clearly stated objectives, including testing system accuracy and potentially testing circumvention techniques.
- Test a representative sample of Australians across different cultures, languages and genders, considering how to cater for those whose lived identity does not match the name or gender on their ID and those who speak languages other than English.
- Provide multiple options for proof of age to help users who do not have access to or feel uncomfortable about a particular method of verification.
- Maintain user privacy by making sure age assurance service providers cannot pass user identity details to website providers and website providers cannot pass to providers information about the content users have accessed.
- Provide participants with options to have granular control over their privacy and offer resources to support their understanding of and informed consent to the sharing of their data, including if and how they may be tracked (for example, through persistent cookies).
- Consider testing tokens stored at the device-level through digital wallets, rather than at the browser level, for user privacy and data security purposes.

- Share resources with euCONSENT and work together on issues of mutual recognition. This includes trialling technologies that have already been accredited as complying with requirements in other jurisdictions, and harmonisation on international standards.

Conclusion

This chapter considers a range of age assurance technologies rather than limiting its assessment to age verification. It demonstrates that there are several methods to determining ages or age ranges in a privacy-preserving and data minimising manner.

There is a desire for stronger controls and safeguards to prevent children's access to age-restricted goods and services but there are strong concerns around trust, transparency and accessibility of the technologies that enable this.

eSafety research found that more than three in four Australian adults, and 91% of young people, support the implementation of age assurance technology by the Australian Government[539], but some respondents reported concerns in the successful design, implementation, and operationalisation of an age assurance or verification system, meaning there is a critical role for public communications and transparency to build good public understanding of these technologies and any applicable quality standards, including privacy and data security requirements.

Many age assurance technologies are still in early stages of development. Further thinking is required around technology design factors, including feasibility, extent and sensitivity of the data required for operation, security and technical integrity, accessibility, barriers to inclusion, and potential for bias. As such, technologies should be further assessed and piloted to determine if they can deliver on the objectives of the roadmap.

Similarly, further thinking is required on implementation factors include transparency and accountability for decision-making, governance and risk management processes, flexibility to account for different business models, compliance with privacy legislation, trustworthiness of the technology, independent oversight, fairness, and equity.

The use of double-blind and zero-knowledge proof systems can facilitate privacy, data security, and user trust. Similarly, device-level technologies, such as tokens and digital wallets, are seen as offering greater control to users and should be considered in future decision-making. The piloting of such technologies in an Australian context would be beneficial to identify gaps and opportunities for their use. Any adopted technologies should be aligned with existing and developing Australian frameworks.

[539] eSafety Commissioner, *Public perceptions of age verification for limiting access to pornography.*

Chapter 9: The enabling environment for age assurance technologies

Key points:

- There is a complex and evolving policy and legislative landscape to consider in implementing any technological measures to prevent and reduce harms associated with children's access to online pornography. This includes existing and emerging international standards, trust frameworks, privacy laws, security guidelines and human and consumer rights protections.
- The elements are at various stages of development. However, they are critical to alleviating stakeholders' concerns about age assurance and satisfying the necessary implementation factors raised in chapter 8, including: the need for independent oversight, strong governance, transparency, trustworthiness, fairness and respect for human rights.
- Policy and legislative developments relating to digital identity and privacy have a particularly important role in informing the development of key safeguards for age assurance.
- To promote international harmonisation, alignment should be sought with relevant international standards which are either in place or under development.
- Should the government support eSafety's recommendation to carry out a pilot, we suggest this should be a cross-government initiative, with digital investment oversight and strategic policy leadership provided by the Digital Transformation Agency, supported by a range of other departments and agencies identified in this chapter which have intersecting equities, remits and workstreams.

Overview

This chapter discusses age assurance and digital identity within the context of the broader enabling environment. This enabling environment consists of various standards, laws, policies, plans, strategies and other initiatives which are relevant to an assessment of the 'implementation factors' set out in chapter 8.

This chapter canvasses the overall age and identity verification landscape in Australia, with a focus on Australia's Digital Identity program. This includes the work of the Digital Transformation Agency (DTA), the recent independent review of myGov and collaboration across states and territories, and the Data and Digital Ministers Meeting.

It also considers existing and emerging international standards which aim to make age assurance systems safe, private, secure and reliable. It highlights considerations that stakeholders and Enex TestLab raised about these standards.

This chapter also explores community attitudes and expectations about privacy (a key theme of the consultations) and outlines relevant protections under the *Privacy Act 1988* (Cth) (Privacy Act) – including how these protections intersect with digital identity developments and reform proposals following the review of the Privacy Act (Privacy Act Review). Finally, developments in data security and human and consumer rights are discussed, with a focus on biometric technologies. Other broader policy developments include the *National Plan to End Violence against Women and Children 2022-2032*, education initiatives around respectful relationships and related topics (see chapter 13), and the classification review (see chapter 14).

The Committee's recommendation tasked eSafety with setting out a suitable legislative and regulatory framework, and program of consultation, for implementing a mandatory age verification regime for online pornography.[540] Stakeholders identified many additional regulatory safeguards which should be built into any proposed regime for mandatory age verification, including the need for age assurance technology providers to be subject to accreditation and oversight to ensure compliance with security standards, privacy protections, and human and consumer rights. Based on our consultations across government, a legislative and regulatory framework for age assurance covering all necessary elements does not yet exist. However, such a framework could be built on the existing foundations of equivalent accreditation regimes in government, such as the Trusted Digital Identity Framework, and strengthened privacy protections arising from the Privacy Act Review (subject to government considerations).

[540] House of Representatives Standing Committee on Social Policy and Legal Affairs, '*Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*', Parliament of Australia, 2020, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report.

International standards and certifications for age assurance

The standards covered in this section are those which set out specifications, procedures and guidelines that aim to make sure products, services and systems are safe, consistent and reliable. Such standards can cover a variety of subjects, including privacy and data protection, security, usability, accessibility and more.

Relevant international standards are developed by bodies such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), the International Telecommunications Union and others for countries to adopt for national use.

In submissions to the Inquiry Committee, there was general support for a standards-based approach to implementing online age verification.[541] The Committee found establishing robust technical standards to be a prerequisite for the implementation of any mandatory age verification regime,[542] and recommended the DTA, in consultation with the Australian Cyber Security Centre (ACSC), develop standards for online age verification for age-restricted products and services in Australia.[543] The previous government's Inquiry response indicated this work would be subject to the findings of this report, as well as the Department of Social Services' review of customer verification requirements for online wagering, discussed later in this chapter.[544]

Stakeholders in eSafety's consultations reiterated the important role of standards in building trust and enabling interoperability across various national ecosystems and frameworks. Our discussions with ACSC, DTA and other government agencies confirmed there was a desire to make sure Australia is working in harmony with standards being developed internationally. This sentiment is echoed in several policy documents such as the Department of Foreign Affairs and Trade International Cyber and Critical Technology Engagement Strategy and Adoption of International Standards Policy.[545]

[541] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, 2020, at para 2.52.

[542] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, 2020, at para 2.137.

[543] House of Representatives Standing Committee on Social Policy and Legal Affairs, 2020, at para 2.143.

[544] Australian Government, '*Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence*', Parliament of Australia, 2021, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Government_Response.

[545] Department of Foreign Affairs and Trade, '*Critical technology standards*', available at: https://www.internationalcybertech.gov.au/our-work/prosperity/critical-technology-standards; Standards Australia, '*Adoption of International Standards*', 2016, available at: https://www.standards.org.au/getmedia/98dfe8c9-4d35-4b14-bcf3-1bfef35e935f/SG-007-Adoption-of-International-Standards.pdf.aspx.

Current and draft international standards

ISO/IEC 27566

The ISO is currently preparing a draft international standard for age assurance systems.[546] This standard, known as 'ISO/IEC 27566 - Information security, cybersecurity and privacy protection - Age assurance systems' - Framework, is technology neutral and seeks to:

- define the key terms, definitions and abbreviations applicable to the age assurance process
- specify requirements for establishing the indicators of confidence associated with age assurance systems (asserted, basic, standard, enhanced, strict) without recommending or requiring particular age assurance thresholds
- specify the roles, responsibilities and procedures of key actors in the age assurance process
- give guidance around countermeasures (i.e., anti-spoofing techniques547)
- specify, at a high level, the data protection, privacy and security requirements specific to the age assurance process.

This standard remains in the 'preparatory' stage of development.[548] Standards Australia, as Australia's national standards body, is a member of the ISO.[549]

PAS 1296 and Age Check Certification (UK)

In 2018, the British Standards Institute and the Digital Policy Alliance published a Publicly Available Specification (PAS) 1296 which contains technical requirements for age check systems. PAS 1296 guides providers of age-restricted products and services to adopt and demonstrate best practice and compliance in age-checking. The standard covers privacy, security, safety, usability, accessibility, and data protection online. Like the draft ISO standard, it is technology agnostic and does not establish thresholds or required levels of confidence in age verification processes.

Compliance with this standard is recommended for members of the Age Verification Providers Association (AVPA), the global trade body for independent providers of age assurance technology. As such, it serves as the current de-facto global standard for age verification.[550]

[546] IsecT Ltd, '*ISO/IEC 27566'*, SecAware, 2022, available at: https://www.iso27001security.com/html/27566.html.
[547] Spoofing refers to the practice of cybercriminals disguising their identity to trick someone into thinking that the cybercriminal is another person or organisation, in order to win that person's trust.
[548] ISO, '*ISO/IEC AWI 27566 Information security, cybersecurity and privacy protection — Age assurance systems — Framework'*, available at: https://www.iso.org/standard/80399.html.
[549] Department of Foreign Affairs and Trade, *Critical technology standards*.
[550] Age Verification Providers Association (AVPA), .*International standards for age verification.,* available at: https://avpassociation.com/standards-for-age-verification/.

It is also the standard applied by the Age Check Certification Scheme (ACCS), a UK Accreditation Service comprised of auditors, certification specialists and data protection experts.[551] ACCS independently tests and certifies online and offline systems that check age and identity against PAS 1296, the ICO's Children's Code (discussed in chapter 10) and/or the UK Government's Digital ID Trust Framework.[552] To determine compliance with PAS 1296, ACCS requires organisations to provide documentation on their approach to age validation, information about their data protection and privacy policies, and quality management system.[553] According to its public register, eight systems have been awarded age assurance certificates: AgeChecked, Innovative Technology, VerifyMyAge, One Account, OndID, Privately, VeriMe and Yoti.[554]

IEEE 2089.1 (US)

In November 2021, the Institute of Electrical and Electronics Engineers (IEEE), a US-based professional body for electronic and electrical engineering, published Standard 2089-2021, which prescribes certain processes to make sure engineers and technologists are considering children's rights through product development.[555] This open-access standard was developed in cooperation with the 5Rights Foundation, a UK-based charity which aims to put children's needs and rights at the heart of digital design.[556] eSafety participated in working group discussions with 5Rights during the development of the standard, and our resources are listed as one of several age-appropriate frameworks which informed the standard.[557]

The IEEE standard encompasses the following key principles:

- recognition that the user is a child
- acknowledgement of the diversity of children and young people
- presentation of information in an age-appropriate way
- utilisation of fair terms appropriate for children
- prioritisation of children's best interests over commercial interests.[558]

[551] Age Check Certification Scheme, *About us*, ACCScheme, available at: https://www.accscheme.com/about.
[552] Age Check Certification Scheme, *About us.*
[553] Age Check Certification Scheme, *FAQ.*
[554] Age Check Certification Scheme, '*Registry*', ACCScheme website, available at: https://www.accscheme.com/registry.
[555] IEEE SA, '*IEEE standard for an age appropriate digital services framework based on the 5Rights Principles for Children*', 5Rights Foundation, 2021, available at: https://5rightsfoundation.com/static/ieee-2089-2021.pdf.
[556] 5Rights Foundation, *5Rights*, available at: https://5rightsfoundation.com/.
[557] IEEE SA, *IEEE standard for an age appropriate digital services framework based on the 5Rights Principles for Children*, 5Rights Foundation, 2021.
[558] IEEE SA, '*IEEE publishes new standard to address age appropriate design for children's digital services*', 2021, available at: https://standards.ieee.org/news/ieee-2089/.

IEEE 2089-2021 aims to address issues related to privacy, safety, trust, security, and usability throughout the life cycle of development, delivery, and distribution of digital products and services.

This standard recommends the use of 'age assurances mechanisms proportionate to the risk and nature' of a product or service. However, it does not include any requirements regarding age assurance technologies or processes.[559]

As of March 2023, a draft trial-use version of 2089.1 Standard for Online Age Assurance (Age Verification and Age Estimation) was awaiting approval by ballot. This working draft provides more detail on the roles and responsibilities of key actors in the age assurance process, determining the need for age verification, selecting the method of age verification, and finally, establishing standard levels of age assurance based on the extent of confidence in the output.

IEEE 2089.1 also recommends activities that could be performed to protect user privacy and ensure secure operations by implementing privacy by design.[560] The new IEEE standard requires age verification providers to document how age verification attempts are recorded to confirm it is not possible for the platform or service requesting the verification of a user to identify the user, and it is not possible for the provider to record which requesting parties enquired about which of its users (i.e., the standard requires providers to document its double-blind method and zero-knowledge proofing).[561]

ISO 31700-1

The Privacy by Design (PbD) framework was introduced in the 1990s by then-Canadian Information and Privacy Commissioner, Dr. Ann Cavoukian.[562] In October 2010, the 32nd International Conference of Data Protection and Privacy Commissioners passed a resolution that recognised Privacy by Design as an essential component of fundamental privacy protection.[563]

In January 2023, ISO published ISO 31700-1 - Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements. This standard establishes high-level requirements for privacy by design to protect privacy throughout the consumer product

[559] IEEE SA, *IEEE standard for an age appropriate digital services framework based on the 5Rights Principles for Children*, 5Rights Foundation, 2021.

[560] Office of the Australian Information Commissioner, '*Privacy by design*', available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/privacy-by-design.

[561] IEEE SA*, 'Compliance with IEEE Standards policies and procedures',* 2021, available at: https://sagroups.ieee.org/2089-1/wp-content/uploads/sites/451/2021/12/IEEE-P2089.1-Draft-Contribution-8-Dec-2021.pdf.

[562] Privacy by Design Centre for Excellence, *Dr Ann Cavoukian*, Toronto Metropolitan University, available at: https://www.torontomu.ca/pbdce/about/ann-cavoukian/.

[563] Global Privacy Assembly*, 'Resolution on Privacy by Design',* 2010, available at: https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

lifecycle, including data processed by the consumer.[564] ISO 31700-1 provides three guiding principles for embedding privacy by design:

- Empowerment and transparency – promoting wider adoption of privacy-aware design, earning consumer trust, and satisfying consumers' need for robust privacy and data protection.
- Institutionalisation and responsibility – the consumer's privacy is considered early and throughout the product lifecycle process by those processing personally identifiable information.
- Ecosystem and lifecycle – applying a privacy by design approach to broader information ecosystems in which both technologies and organisations operate and function.

ISO has also published a complementary technical report (ISO/TR 31700-2) which provides descriptive use cases, with associated analysis, to help readers understand the requirements of 31700-1.[565]

European Commission standard on age assurance/age verification

Under the new European strategy for a Better Internet for Kids, the European Commission has committed to issuing a standardisation request for a European standard on age assurance/age verification by 2024.[566]

The standard is intended, among other things, to clarify what is expected from the online industry when age verification is required on any online tools and services, including to restrict online pornography.[567]

Considerations for standards development, implementation and auditing

While there was general agreement in our consultations that international standards can play an important role in setting baseline requirements, promoting user trust, and facilitating interoperability, stakeholders also raised some concerns. These included perceived or actual conflicts of interest among participants in the standards-making process who may have business interests in the adoption of particular safety technologies. Stakeholders urged inclusive, multi-disciplinary input and a technology-neutral approach which could be applied to a wide variety of existing and emerging technologies.

[564] ISO, '*ISO 31700-1:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*', 2023, available at: https://www.iso.org/standard/84977.html.

[565] ISO, '*ISO/TR 31700-2:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases*', 2023, available at: https://www.iso.org/standard/84978.html.

[566] European Commission, '*New European strategy for a better Internet for kids*', 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2826.

[567] European Commission, *New European strategy for a better Internet for kids*, 2022.

Some stakeholders suggested any age assurance regime should be non-prescriptive about standards, whereas others felt standards should be incorporated into Australian law. Some stakeholders felt mutual recognition of national standards should be a focus for regulators. Stakeholders also discussed product accrediting and auditing processes. Privacy experts highlighted the importance of continuously iterating and improving standards over time and conducting ongoing product auditing to identify and mitigate risks to data security.

Some felt the relevant regulator should not inspect every accredited service or product, but rather should be the backstop to third party auditing, the cost of which should be absorbed by the online industry. Government was seen as playing an important role in educating consumers and confirming that age assurance service providers are legitimate, can be trusted, and meet the government's minimum standards.

> 'As a user, I'd want to know that the tool had been rigorously tested to be accurate for people of all ethnicities and genders, minimising bias as much as possible. I think there'd be plenty of people who would also be interested in accessing the training data, as this can tell us lots about how the tool could be making its decisions. Even if it was only made available to researchers or journalists, having the training set available to the public builds trust in the system' – eSafety Youth Council member

Enex TestLab concluded current published standards are not comprehensive but provide helpful high-level guidance. It highlighted that accurate, reliable and reproducible methods for assessing vendor product compliance and comparative baseline benchmarking is required. This is consistent with the findings of a 2021 5Rights Foundation report, which found that:

> '...there are many well-intentioned players in the age assurance space who are developing effective, privacy-preserving and rights-respecting tools for services to know the age of their user...unfortunately, without the standards in place to benchmark or assess the efficacy of solutions, and without a coherent regulatory framework, the ecosystem of age assurance is little more than a sea of known unknowns'.[568]

Within the Australian context, Enex TestLab noted any age assurance regime should be aligned with DTA's Trusted Digital Identity Framework.

[568] 5Rights Foundation, '*But how do they know it is a child? Age Assurance in a Digital World*', 2021.

Age and identity verification in Australia

As identity documents provide a high assurance way to verify age, identity and age verification are often linked, and many of the providers of identity verification services also provide options for age assurance. For example, the providers discussed in chapter 8 offer a combination of age assurance and digital identity solutions drawing on multiple options, including various forms of ID checks.

The extent to which access to age-restricted content or services may also require identity verification depends on the circumstances. In contexts of online wagering and banking, there may be Know-Your-Customer (KYC) requirements which require services to collect and verify both age and identity information.[569]

However, in the context of accessing online pornography, or creating accounts on other online services such as social media, services would only need to establish that a person meets minimum age requirements. Most of the stakeholders we consulted considered that any age assurance regime mandated in Australia should not require online services like pornography sites to collect and store the personal information of their users, given the risk this presents to privacy and security.[570]

As demonstrated through the euCONSENT pilot discussed in chapter 8, it is possible to leverage a single, interoperable age assurance system across multiple use cases requiring different levels of assurance. In addition to streamlining the age checking process for consumers and businesses, this can also reduce the potential stigma it may carry if its use is only associated with accessing pornography. Establishing one system that applies across a range of age-restricted services and products could also provide efficiencies for government as it seeks to address a range of different risks to children.

Through the development of a charging framework, it could potentially reduce the costs borne by regulated industries or entities with fewer resources by distributing those costs across multiple industries. This would go towards meeting several of the implementation factors set out in chapter 8, including flexibility to account for different business models and proportionality to the risks of harm.

It is important to build on lessons learned through trials and consideration of such systems in other contexts. Accordingly, this section explores other Australian developments in relation to online age and identity verification to inform our approach.

[569] ACMA, *'Compliance considerations'*, available at: https://www.acma.gov.au/compliance-considerations; AUSTRAC, *'Customer identification: Know your customer (KYC)'*, available at: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc.

[570] See Appendix 5.

Online Wagering

The National Consumer Protection Framework (National Framework) for online wagering was established in late 2018 by Commonwealth, state, and territory governments. The Department of Social Services (DSS) is responsible for addressing the risks and harms posed by online wagering and leads implementation of the National Framework. The National Framework aims to reduce the harm of online wagering to Australian consumers by removing inconsistencies and associated compliance burdens between Commonwealth, state and territory-based regulations, and making sure strong minimum protections are available to consumers of interactive wagering services. These protections include a national self-exclusion register being developed by the Australian Communications and Media Authority called BetStop – the National Self-Exclusion Register™ that will enable people to ban themselves from all online gambling companies and stop receiving wagering promotions.[571] The Customer Verification measure under the National Framework specifies the allowable timeframe for verification of a customer's identity by an online wagering provider. Customer identity verification is required to register with the national self-exclusion register, as well as to comply with requirements in place under anti-money laundering and counterterrorism financing legislation to verify a user's name, address and date of birth.[572]

Reporting entities under the Anti Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), including organisations providing online wagering services, can rely on third parties to undertake customer identification and verification procedures under defined circumstances.[573] Third parties are not required to undertake accreditation, but they are subject to Part A of the AML Rules, which require them to develop and document procedures to identify, mitigate and manage money laundering and terrorism financing risks their organisation might reasonably face.[574]

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 customer pre-verification or instant 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

[571] Department of Social Services, '*Gambling reform's*, available at: https://www.dss.gov.au/communities-and-vulnerable-people-programs-services-gambling/gambling-reforms; ACMA, '*BetStop – the National Self-Exclusion Register™: FAQs*', available at: https://www.acma.gov.au/betstop-national-self-exclusion-registertm-faqs.
[572] AUSTRAC, *Customer identification: Know your customer (KYC).*
[573] AUSTRAC, '*Reliance on customer identification procedures by a third party*', available at: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/reliance-customer-identification-procedures-third-party.
[574] Australian Government, '*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* at 8.1.7', available at: https://www.legislation.gov.au/Details/F2022C00958.

outcomes of this review should inform next steps for any age assurance regime introduced for online pornography.[575]

Online Alcohol Sales

In November 2020, the New South Wales (NSW) Liquor Act 2007 and Liquor Regulation 2018 were amended to regulate same-day delivery of liquor services. Division 1B sets out provisions relating to age verification processes of this framework.

Currently, a delivery provider has three options to verify a purchaser's age. These include:

- using an identity service provider accredited under the Trusted Digital Identity Framework (explained in the next section)
- using a process that relies on an AI system to authenticate the purchaser's evidence-of-age document
- using self-declaration.576
- The latter two options are initially available only until 31 May 2023, with a review to be conducted by that date.

NSW is also piloting the use of its Service NSW app as proof-of-age for alcohol purchases, enabling users to confirm they are over 18 without providing extra information to alcohol retailers.[577] Further trials involving the Service NSW app are commencing in April 2023, including digital birth certificates.[578] While not everyone holds a birth certificate, most children in Australia have one, as is their right.[579] Digitising birth certificates therefore has the potential to open a more widely accessible avenue for verifying children's age.

Online Safety and Privacy

In December 2021, the House Select Committee on Social Media and Online Safety was established to conduct an Inquiry into Social Media and Online Safety. The Inquiry examined

[575] Australian Government, *Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence,* Parliament of Australia, 2021.
[576] NSW Liquor and Gaming, '*Same day delivery age verification requirement*', 2022, available at: https://www.liquorandgaming.nsw.gov.au/resources/same-day-delivery-age-verification-requirements.
[577] J Bajkowski, '*Dominello prepares to pop cork on digital identity for liquor*', The Mandarin, 2023, available at: https://www.themandarin.com.au/210378-dominello-prepares-to-pop-cork-on-digital-identity-for-liquor/.
[578] R Chirgwin, '*NSW digital birth certificate to be trialled in April*', ITNews, 2023, available at: https://www.itnews.com.au/news/nsw-digital-birth-certificate-to-be-trialled-in-april-591391.
[579]P Gerber and M Castan, '*The right to universal birth registration in Australia*', Get in The Picture: Civil Registration and Vital Statistics in Asia and the Pacific, available at: https://getinthepicture.org/resource/right-universal-birth-registration-australia-melissa-castan-paula-gerber.

'existing identity verification and age assurance policies and practices and the extent to which they are being enforced' on social media services.[580]

Submissions to the Inquiry offered mixed views, with some arguing that privacy-preserving age assurance systems are integral to children's online safety and best interests.[581] Others expressed concerns about privacy and security, as well as scepticism about effectiveness, in efforts to confirm users' age or identity.[582]

One Committee recommendation was the implementation of a mandatory requirement for all digital services with a social networking component to set the highest privacy and safety settings by default for all users under 18 years of age. This would require services to understand their users' age. The Australian Government's response, released in March 2023, points to the Privacy Act Review and its proposal for a Children's Online Privacy Code which would govern how social media and digital platforms use children's data. It notes that such a code would clarify the principles-based requirements of the Privacy Act in more prescriptive terms, including assessing a child's capacity, establishing their age, and applying default privacy settings.[583]

[580] Parliament of Australia, *Inquiry into social media and online safety: Terms of reference*, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Terms_of_Reference.

[581] See submissions from Alannah & Madeline Foundation, Reset Australia, Save the Children, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Submissions.

[582] See submission from Family Zone, Digital Rights Watch, Google, SBS, Australia's Community Manager, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Submissions.

[583] Australian Government, '*Australian Government response to the House of Representatives Select Committee on Social Media and Online Safety report'*, DITRDCA, 2023, available at: https://www.infrastructure.gov.au/sites/default/files/documents/australian-gov-response-to-house-of-reps-select-committee-on-social-media-and-online-safety-report-march2023.pdf.

Digital identity systems in Australia

Digital Transformation Agency and the Digital Identity System

The DTA is responsible for strategic and policy leadership on whole-of-government and shared information and communications technology investments and digital service delivery. This includes Australia's Digital Identity system. Since 2015, the Australian Government has been developing a Digital Identity system that will provide individuals with a simpler, safer and more secure way to verify their identity online.[584]

DTA's Trusted Digital Identity Framework (TDIF) provides the tools, rules and accreditation criteria to protect Australia's Digital Identity System. The TDIF specifies the minimum standards entities must meet to become a part of the system. This includes security, privacy, accessibility, usability, service operations and technical integration matters.

The TDIF has been developed, and is continuously iterated, in collaboration with key stakeholders including government agencies, peak industry bodies, privacy commissioners, state and territory governments and the wider public. It is also consistent with international standards such as ISO standards, OpenID Connect, Security Assertion Markup Language, FIDO Biometrics Framework and NIST Digital Identity and Authentication standards.[585]

The Digital Identity System is comprised of four types of accredited participants:

- **Identity providers** – who help people set up and manage their Digital Identity account, serving as a gateway into the Digital Identity system. Examples of identity providers are myGovID and Australia Post's Digital ID service.
- **Attribute service providers** – who are entities such as professional bodies or universities that can provide, with a person's consent, authoritative information about an attribute they have, such as a degree or qualification.
- **Credential service providers** – who play a critical role in keeping the system secure and safe. They take care of all credentials (that is, passwords and other forms of access restrictions) used in the system.
- **An identity exchange** – which facilitates interactions between accredited participants to occur in a way that is secure and privacy-respecting. The identity exchange acts like a switchboard: transferring information, with a person's consent, between relying parties, identity service providers and attribute service providers. The identity exchange only passes on the specific information which the person consents to be shared – nothing

[584] Digital Transformation Agency, *Digital Identity legislation: Background paper*, Digital Identity System, 2020, available at: https://www.digitalidentity.gov.au/previousconsultations.
[585] Digital Transformation Agency, *Digital Identity legislation: Background paper*, 2020.

more, nothing less. In this way, the identity exchange incorporates privacy by design and helps protect personal information.

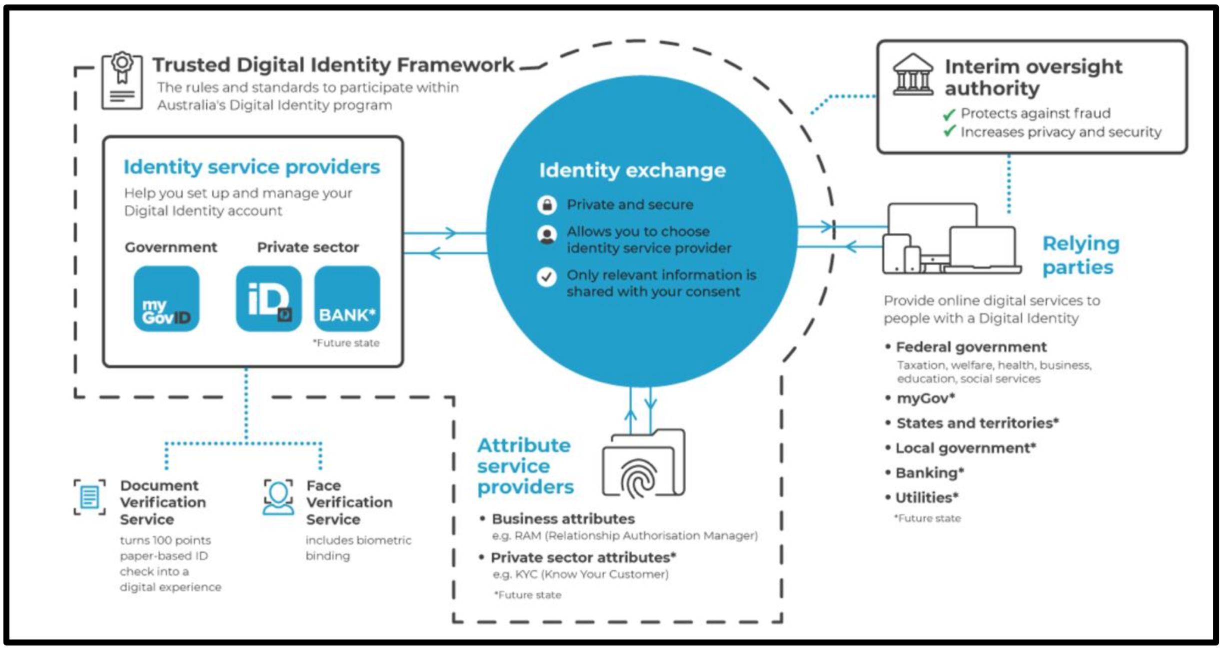

Trusted Digital Identity Framework
The rules and standards to participate within Australia's Digital Identity program
Identity service providers
Help you set up and manage your Digital Identity account
Government
Private sector
myGovID
iD
BANK*
*Future state
Identity exchange
Private and secure
Allows you to choose identity service provider
Only relevant information is shared with your consent
Interim oversight authority
✓ Protects against fraud
✓ Increases privacy and security
Relying parties
Provide online digital services to people with a Digital Identity
• Federal government
Taxation, welfare, health, business, education, social services
• myGov*
• States and territories*
• Local government*
• Banking*
• Utilities*
*Future state
Document Verification Service
turns 100 points paper-based ID check into a digital experience
Face Verification Service
includes biometric binding
Attribute service providers
• Business attributes
e.g. RAM (Relationship Authorisation Manager)
• Private sector attributes*
e.g. KYC (Know Your Customer)
*Future state

Figure 14 Australia's Trusted Digital Identity Framework

There are different identity-proofing levels within the TDIF which are closely aligned to the Department of Home Affairs' National Proofing Guidelines. Lower level, or basic identity proofing has minimal requirements, such as an email address or mobile phone number and one identity document. Standard identity proofing requires two documents, such as a driver licence and passport. Strong identity proofing requires two documents, at least one of which has a photo, accompanied by a face scan to match against the photo.[586] A user's face scan and documents are deleted as soon as their identity is confirmed.[587]

Trusted Digital Identity Legislation and Regulatory Oversight

In 2020, the DTA released a consultation paper seeking views on key principles to guide the development, design, scope and content of Australia's Trusted Digital Identity legislation.[588] It was proposed that this legislation would:

- allow states, territories and the private sector to participate in the Digital Identity System
- enshrine privacy and consumer protections, so users can have confidence their personal information is safe and secure

[586] Digital Identity System, '*What are identity proofing levels?*', available at: https://www.digitalidentity.gov.au/about/what-are-identity-proofing-levels.

[587] myGov ID, '*Verifying your photo*', available at: https://www.mygovid.gov.au/help-proving-your-identity#verifying-your-photo; myGov ID, '*Privacy policy: How we hold personal information*', available at: https://www.mygovid.gov.au/mygovid-privacy-policy#Howwehold.

[588] Digital Transformation Agency, '*Digital Identity legislation: Consultation paper*', Digital Identity System, 2020, available at: https://www.digitalidentity.gov.au/previousconsultations

- establish governance arrangements and strong regulation for organisations that provide services in the system (such as identity or attribute providers) to further protect users
- expand TDIF accreditation to other governments and the private sector.

These proposals aimed to provide users and businesses with a market of certified service providers and establish a redress scheme so users would have protection in the event of fraud or a cyber security incident.[589] Stakeholders who took part in the DTA's subsequent consultations noted the importance of good governance, privacy protection, clarity of liability in case of a breach, interoperability between Australia's Digital Identity System and other systems, and the need for digital identity to be voluntary.[590] In response, the DTA added a new interoperability principle, as well as the right to deregister and use an alternative channel to Digital Identity if desired.[591]

In October 2021, the previous Australian Government released an exposure draft of the Trusted Digital Identity Bill 2021 (Cth) and related legislative instruments.[592] Following a change of government, it is anticipated that new legislation will be introduced to Parliament in the second half of 2023. This will include the appointment of a regulator to provide oversight of accredited entities. In the meantime, the Australian Government has begun accrediting businesses under the TDIF, such as eftpos (September 2021)[593] and Mastercard (June 2022),[594] as it readies itself for the Digital Identity System to expand beyond Commonwealth agencies to the private sector.

Like digital identity, the establishment of a regulatory scheme for age assurance providers would need to contemplate applicable minimum standards, governance and risk management processes, transparency and accountability mechanisms, and privacy and human rights protections. It would also need to involve 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

[589] Digital Identity System, Legislation consultation: Phase 3, Digital Identity System website, 2021.
[590] Digital Identity System, Legislation consultation: Phase 3, 2021.
[591] DTA, '*Digital Identity legislation position paper summary*', DTA website, 2021.
[592] Digital Identity System, Legislation consultation: Phase 3, Digital Identity System website, 2021.
[593] Minister for Employment, Workforce, Skills, Small and Family Business, '*eftpos accredited as first private identity exchange under Trusted Digital Identity Framework*', Ministers' Media Centre, 2021, available at: https://ministers.dese.gov.au/robert/eftpos-accredited-first-private-identity-exchange-under-trusted-digital-identity-framework
[594] Digital Identity System, '*Mastercard achieves TDIF accreditation for three roles*', 2022, available at: https://www.digitalidentity.gov.au/news/mastercard-achieves-tdif-accreditation-for-three-roles.

- any enabling IT infrastructure for the regulatory regime
- general regulatory functions – reporting, publication of guidance, etc.

Based on interdepartmental discussions, there is likely no existing regulator or accreditation body that has the full breadth of experience and capability to provide all necessary functions, particularly in relation to this type of digital accreditation.

The Committee that gave rise to this report recommended the DTA extend the Digital Identity program to include an age verification exchange for the purpose of third-party online age verification.[595] The previous Australian Government supported this recommendation in principle, subject to the outcomes of other ongoing processes, including the development of this report. As highlighted in the DTA's evidence to the Committee, such an extension would require further investment and amendments to the forthcoming legislation.

Based on our stakeholder consultations and our review of the enabling environment in Australia, eSafety would support building on the work of equivalent regimes in government, such as the TDIF and related forthcoming legislation, as a good basis for starting discovery work on how an accreditation and oversight scheme for age assurance providers could operate. Accordingly, the DTA is an essential stakeholder in any pilot or mandate involving age assurance.

Differentiating between Australia's Digital Identity system and age assurance

It is important to differentiate between extending the Digital Identity System to cover the accreditation of private providers of age assurance technology and extending the use of the Australian Government's identity app, myGovID, to establish a user's age for purposes of accessing pornography. While the DTA's evidence to the Committee confirmed Digital Identity could be used to verify a user's age for purposes of accessing online pornography in a privacy-preserving way, the DTA recommended that if Digital Identity is to be used for age assurance, it should be one of many options and not the only avenue. eSafety supports this, as there is likely to be a level of public discomfort in using myGovID as the sole mechanism for accessing pornography. Building on similar work being undertaken in Europe (see chapter 8), users should have the option to choose between multiple third-party age assurance providers, ideally through a double-blind exchange.

[595] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, 2020.

myGov Audit and acceleration of digital identity

In September 2022, the Minister for Government Services commissioned a panel of experts, including the eSafety Commissioner, to review myGov, which enables account holders to access government services. The review considered how well myGov is performing for Australians when it comes to reliability, functionality and delivering a user-friendly experience.[596] Noting that recent cyber breaches have reinforced underlying citizen concerns about security and privacy, the review placed particular emphasis on the importance of trust and fairness, which were also major themes of eSafety's stakeholder consultations for this report.[597]

The panel delivered their audit in January 2023, making 10 recommendations to the Australian Government, including to 'accelerate the development of Australia's national digital identity ecosystem, prioritising the protection of security, privacy, safety and other human rights with a view to government digital identity being safe, easy to use and secure'.[598] If achieved, an enabling environment with these qualities would satisfy many of the implementation factors set out in chapter 8 and address most concerns raised by stakeholders in our consultations.

The panel's roadmap planned for a national framework for the interoperability of credentials across jurisdictions to be implement by late 2023 and for digital identity attribute providers to be introduced by mid-2024 to make linking to services easier. The Australian Government will provide a full response to the report later in 2023.

Interoperability and trust in digital identity

- Organisations including the eIDAS in Europe, Pan-Canadian Trust Framework in Canada and Aadhaar in India are working towards interoperability and trust in digital identity. A trust framework is a common set of standards-based rules which make sure minimum requirements are met for privacy, security, interoperability, governance, and accreditation.
- The Open Identity Exchange (OIX) is a non-profit organisation that has also been working to address this issue since 2015. OIX advocates for the transparent description of the characteristics of trust framework policies to allow global consistency and interoperability.
- OIX is working on defining and disseminating these minimum characteristics as part of its Global Interoperability and its Trust Framework Principles, Trustmark and Governance working groups. The aim of these groups is to publish a high-level guide

[596] myGov, '*myGov user audit*', 2023, available at: https://my.gov.au/en/audit.
[597] myGov, 'Critical National Infrastructure: myGov user audit – Volume 1', myGov, 2023, available at: https://my.gov.au/en/audit.
[598] myGov, Critical National Infrastructure: myGov user audit – Volume 1, 2023.

for Trust Frameworks through analysis of different regional frameworks and determine what is needed to allow IDs from one framework to be accepted in another.

- In alignment with these international developments, the importance of interoperability for international harmonisation was highlighted by stakeholders in our consultations and emphasised by Enex TestLab.

Data and Digital Ministers Meeting

The Data and Digital Ministers Meeting is chaired by Senator the Hon Katy Gallagher, Minister for Finance, Minister for the Public Service, Minister for Women, representing the Commonwealth. It includes ministerial representation from all Australian states and territories and also New Zealand. The purpose of this forum is to achieve cross-government collaboration on data and digital transformation to ensure smarter service delivery and improved outcomes.[599]

Data and Digital Ministers are working to align policies and services across Australia by:

- reforming cross-jurisdictional data and digital platforms, services and protocols
- enhancing government capability to build public trust and deliver digital services
- delivering a seamless digital identity experience for citizens
- transforming government services around life events.

The Data and Digital Ministers tasked Home Affairs (as the Commonwealth lead on identity security), to work with states, territories and other Commonwealth agencies to develop the National Strategy for Identity Resilience (the Identity Resilience Strategy). The Identity Resilience Strategy seeks to coordinate a national approach to identity and make identities harder to steal, and if compromised, easier to restore. It looks to address the growing need to protect the identities of Australians from identity-related crime particularly following high-profile data breaches in 2022. One way it seeks to do this, is by committing to reducing the collection and retention of data and to using the minimum personal information needed for a transaction. In February 2023, Ministers endorsed in-principle a draft strategy, with a final strategy to be considered later this year.[600]

Ministers also agreed at the February 2023 meeting to explore ways to support the National Plan to End Violence against Women and Children 2022-2032 (the National Plan).[601] To this end,

[599] Department of Finance, '*Data and digital ministers meeting*', available at: https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting.

[600] Department of Finance, '*Data and digital ministers meeting communiqué – 24 February 2023*', 2023, available at: https://www.finance.gov.au/publications/data-and-digital-ministers-meeting-outcomes/24-february-2023.

[601] Commonwealth of Australia, ''*National Plan to End Violence against Women and Children 2022-2032*', Department of Social Services, 2022. https://www.dss.gov.au/ending-violence.

they committed to working with Women's Safety ministers to identify opportunities to improve data sharing.[602] The National Plan makes a connection between children's access to online pornography and harmful attitudes and behaviours towards women. Engagement with Data and Digital Ministers on age assurance measures to prevent such access will provide a further opportunity for them to contribute to whole-of-government efforts to combat violence against women.

Digital inclusion was also discussed at the February 2023 meeting. Ministers agreed to continue collaborating to support the digital inclusion of First Nations people, women and those of diverse backgrounds.[603] As explored in chapter 8, inclusion and accessibility will be a key element to any age assurance regime, as will privacy. 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 will be a critical stakeholder in any pilot or mandate involving age assurance.

[602] Department of Finance, *Data and digital ministers meeting communiqué – 24 February 2023*, 2023.
[603] Department of Finance, *Data and digital ministers meeting communiqué – 24 February 2023*, 2023.

Privacy

Making sure the privacy of Australians is appropriately protected and regulated in an ever-changing digital world is a key priority across the community, government and industry. As highlighted in chapter 4, privacy is a fundamental human right, which must be protected within any age assurance regime, in conjunction with other human rights. As emphasised in chapter 8, it is critical to fostering trust and confidence in data handling activities.

Stakeholder consultation

The need to respect privacy, and to have robust measures in place to mitigate against privacy risks and harms, was raised consistently across multiple stakeholder groups eSafety consulted in the development of this report.

Stakeholders spoke about the potential for data breaches and privacy invasions, and some considered that there was a point at which the risk of unintended privacy consequences for the community – including children – could outweigh the beneficial impacts of preventing children's access to pornography.

Some felt strongly that age assurance measures should not be linked to other identity systems, noting potential intersections with broader movements to identify people on the internet. They raised concerns in relation to the normalisation of surveillance and the risk of re-identification of users from seemingly anonymous data sets. Some stakeholders also felt current legislation to protect individuals' privacy may be inadequate.

Stakeholders recommended a variety of ways to address these concerns, including:

- taking a data-minimisation approach to age assurance
- requiring age assurance technology providers to be transparent about their systems and processes, and how they adhere to privacy and security standards
- providing clear consequences for data breaches or other misuse or mishandling of data, as well as accessible and affordable legal avenues for individual and collective rights of action against privacy breaches
- making sure any age assurance scheme is not 'set and forget', with privacy and security risks continually reviewed and iterated
- designing friction into the legislative process to reduce the potential for age assurance measures to be expanded over time, as well as a review period and/or sunsetting provision.

Community attitudes

In addition to eSafety's public perceptions and youth focus group research findings (see chapter 5), the Office of the Australian Information Commissioner (OAIC) conducted the Australian Community Attitudes to Privacy Survey (ACAPS, 2020).[604] This provided insights about the community's broader privacy concerns. The survey reveals privacy is a major concern for 70% of Australians, and almost 9 in 10 want more choice and control over their personal information. Privacy is now a top consideration when choosing a digital service – ahead of reliability, convenience, and price.

Importantly, comfort with certain data practices depends on the type of information collected, the purpose behind it, and the level of trust in the organisation involved. The Australian community expressed strong views on the collection and potential misuse of personal information – including being asked for information that does not seem relevant or being unknowingly tracked on websites. Compared to the 2017 results, in 2020 individuals were more likely to take certain actions to protect their privacy, such as deleting an app, denying permission to access information and clearing browser history.

According to research commissioned by the Digital Industry Group Inc (DIGI) in September 2022, 42% of respondents said they did not trust governments with their private data and information, and 47% said they did not trust private digital companies with this data.[605] These insights and concerns from the community are currently informing the review of the Privacy Act.

The Privacy Act 1988 (Cth)

The Privacy Act regulates the handling of 'personal information'[606] by Australian Government agencies and organisations with an annual turnover of more than $3 million, as well as certain smaller organisations (known as 'APP entities').[607] Notably, the TDIF provides that accredited

[604] Office of the Australian Information Commissioner, '*Australian community attitudes to privacy survey*', 2020, available at: https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020.

[605] Resolve, '*Consolidated industry codes of practice for on-line class 1 content: Community research (Commissioned by Digital Industry Group Inc and Communications Alliance)*', Online Safety, 2022, available at: https://onlinesafety.org.au/submissions/.

[606] Personal information is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not'. Source: Office of the Australian Information Commissioner (OAIC), *What is personal information?,* 2020, available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information.

[607] Some organisations with an annual turnover of $3 million or less are also subject to the Privacy Act. For more information, see OAIC guidance on responsibilities under the Privacy Act: Office of the Australian Information Commissioner (OAIC), *Rights and responsibilities*, available at: https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities.

entities must abide by the Privacy Act or a state or territory law providing an equivalent level of protection.[608]

The Privacy Act contains 13 legally binding Australian Privacy Principles (APPs) which contain privacy obligations across the information life cycle as entities collect, hold, use, disclose, destroy or de-identify personal information. The APPs are technology-neutral and provide entities with the flexibility to take a risk-based approach to compliance, based on their circumstances (e.g., size, resources and business model) while ensuring the protection of individual's privacy. The Privacy Act and the APPs apply equally to the personal information of adults and children and do not specify an age at which individuals can make their own privacy decisions.

The OAIC's APP Guidelines provide guidance to entities on the meaning of consent for the purposes of the Privacy Act[609]. The guidelines state that consent contains four elements – the individual must be adequately informed before giving consent, the individual must give their consent voluntarily, the consent must be current and specific, and the individual must have the capacity to understand and communicate their consent. The Guidelines provide that an APP entity may presume an individual has the capacity to consent if they are 15 years or older, unless they are unsure. The Attorney-General has proposed a series of reforms to the Privacy Act to strengthen the protection of personal information and the control individuals have over the information. Consideration will need to be given to the potential interaction between these reforms and any age assurance pilot or mandate flowing from this report. The APPs provide that:

- APP entities must handle personal information in an open and transparent way, including by having a clearly expressed and up-to-date privacy policy (APP 1).
- Individuals must be given the option of not identifying themselves or of using a pseudonym unless an exception applies (APP 2).
- Personal information must only be collected when it is reasonably necessary for an entity's functions or activities (APP 3). Heightened protections apply for the collection of sensitive information.[610]

[608] Australian Government, '*Digital Identity functional requirements: Trusted digital identity framework release 4.8'*, Digital Identity System, 2023, available at: https://www.digitalidentity.gov.au/sites/default/files/2023-03/tdif_04_functional_requirements_-_release_4.8.pdf.

[609] Office of the Australian Information Commissioner, *'Australian Privacy Principles guidelines – Chapter B: Key Concepts'*, 2022, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines.

[610] Sensitive information is defined in section 6 of the Privacy Act as information of an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or membership of a trade union, sexual orientation or practices or criminal record that is also personal information, health information about an individual, genetic information about an individual, biometric information that is to be used for the purpose of automated biometric verification or identification, or biometric templates.

- Entities must take reasonable steps to ensure individuals are notified of certain matters when personal information is collected, including information about the entity collecting the information, the purposes for which it is collected, any other entities to whom the personal information may be disclosed (including overseas) etc. (APP 5).
- Personal information must not be used or disclosed for a purpose other than the primary purpose unless the individual consents, or an exception applies (APP 6).
- Limitations and obligations regarding the use or disclosure of personal information for direct marketing purposes (APP 7), cross-border disclosures (APP 8) and adoption, use or disclosure of government-related identifiers (APP 9).
- APP entities must take reasonable steps to ensure personal information collected is accurate, up to date and complete (APP 10).
- APP entities must take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP entities must also destroy personal information once it is no longer needed (APP 11).
- APP entities must give individuals access to the personal information they hold about that individual on request (APP 12) and must correct personal information that is inaccurate, out of date, incomplete, irrelevant or misleading (APP 13).

The APPs are subject to certain exceptions. Additionally, APP entities have obligations under the Notifiable Data Breaches (NDB) scheme (set out in Part IIIC of the Privacy Act) to notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Privacy Act review

The Attorney-General's Department (AGD) commenced the Privacy Act Review in October 2020, following the Australian Competition and Consumer Commission's 2019 Digital Platforms Inquiry Final Report. The review has considered whether the Privacy Act and its enforcement mechanisms are fit for purpose in an environment where Australians now live much of their lives online and their information is collected and used for a myriad of purposes in the digital economy. In October 2020, an initial issues paper[611] was released by the AGD, followed by a discussion paper in October 2021[612].

On 16 February 2023, the Government released the AGD's Privacy Act Review Report.[613] The Report makes 116 proposals for reforms, which are designed to better align Australia's laws with global standards of information privacy protection and properly protect Australians' privacy. The Government is considering feedback on the Report, which will be used to inform the Government's response to the report that sets out the pathway for reforms.

The proposals put forward in the report are intended to increase and uplift the privacy protections for all individuals (regardless of age), as well as provide some targeted privacy protections for children. Proposals that would likely uplift and increase the protection of personal information generally (including for children and people experiencing vulnerability) include:

- Amending the definition of 'personal information' to clarify it is intended to cover technical information (e.g., IP address and location data) where that information relates to an individual,614 and clarifying that 'collection' includes information obtained from any source and by any means, including inferred or generated information.[615]
- Introducing a requirement that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances, including consideration of whether an individual would reasonably expect the handling of the personal information, or whether it was reasonably necessary for the functions or activities of the organisation to collect and use the information.[616]

[611] Attorney-General's Department, *'Review of the Privacy Act 1988 (Cth) – Issues Paper'*, AGD website, 2020, https://www.ag.gov.au/rights-and-protections/publications/review-privacy-act-1988-cth-issues-paper.

[612] Attorney-General's Department, '*Privacy Act Review – Discussion Paper*', AGD website, 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

[613] Attorney-General's Department*, 'Privacy Act Review – Report'*, AGD website, 2022, https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

[614] Privacy Act Review – Report, Proposal 4.1.

[615] Privacy Act Review – Report, Proposal 4.3.

[616] Privacy Act Review – Report, Proposal 12.1.

- Introducing a requirement for all APP entities to conduct a Privacy Impact Assessment for activities with high privacy risks and considering enhanced risk assessment requirements for facial recognition technology and other uses or biometric information.[617]
- Introducing additional rights of the individual, including a right to receive an explanation of what an APP entity has done with personal information, a right to object to collection, use or disclosure of personal information, a right to erasure (request information be deleted), and a right to de-index online search results in certain situations.
- Promoting consistent uptake of foundational cyber security controls and standards across the economy, and data minimisation by:
    - requiring entities to consider technical and organisation measures to protect personal information and comply with a set of baseline privacy outcomes[618]
    - keep de-identified information secure given the risk or re-identification[619]
    - establish how long they will retain personal information having regard to the nature, sensitivity and purpose of that information and periodically review[620]
    - enhanced OAIC guidance on what reasonable steps an entity should take to keep personal information secure, and steps to destroy or de-identify information.[621]

The Report also contains proposals that relate specifically to children and seek to enforce a higher level of privacy protection for this group. This includes:

- Specifying that, in determining whether a collection, use or disclosure is 'fair and reasonable in the circumstances', the best interests of the child should be considered, among other matters.[622]
- Introducing a requirement for collection notices and privacy policies to be clear and understandable, in particular for any information addressed specifically to a child.[623]
- Prohibiting or restricting certain practices, including direct marketing to a child, targeting to a child, and trading in the personal information of a child, unless it is in their best interests.[624]
- Introducing a Children's Online Privacy Code that applies to online services 'likely to be accessed by children'.[625] The report suggests that to the extent possible, the

[617] Privacy Act Review – Report, Proposals 13.1 and 13.2.
[618] Privacy Act Review – Report, Proposal 21.1 and 21.2.
[619] Privacy Act Review – Report, Proposal 4.6 and 21.4.
[620] Privacy Act Review – Report, Proposal 21.7.
[621] Privacy Act Review – Report, Proposal 21.3 and 21.5
[622] Privacy Act Review – Report, Proposal 12.2 and 16.4.
[623] Privacy Act Review – Report, Proposal 16.3.
[624] Privacy Act Review – Report, Proposals 20.5, 20.6 and 20.7.
[625] Privacy Act Review – Report, Proposal 16.5.

scope of an Australian Children's Online Privacy Code should align with the scope of the UK Age-Appropriate Design Code, discussed in chapter 10. Public feedback on the report will inform the Government's next steps.

- Requiring that valid consent must be given with capacity, and existing OAIC guidance on children and young people and capacity should continue to be relied on by APP entities.[626] That is, an entity must decide if an individual under the age of 18 has the capacity to consent on a case-by case basis.[627] If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

According to the Report, 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, requirements in relation to 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, and balancing parental controls with a child's right to autonomy and privacy. This would have implications for age assurance and other safety measures to prevent harm to children from online pornography.

As raised in eSafety's submission to the previous Australian Government's draft Online Privacy Bill, it is our view that requiring online services to conduct different age assurance processes for purposes of data collection and online safety would be onerous, duplicative and confusing for industry and consumers.[628] We believe an age assurance pilot, as recommended in this report, could inform a coordinated and privacy-preserving approach to determining users' age for a range of purposes, including to prevent children's encounters with online pornography as well as to establish a child's age for the purposes of complying with a Children's Online Privacy Code, if implemented. This approach is supported by the Privacy Act Review Report.[629] Should the government support eSafety's recommendation to carry out a pilot and the relevant recommendations in the Privacy Act Review Report, we suggest the pilot should involve AGD and OAIC, and must include a Privacy Impact Assessment. Chapter 10 explores how online safety and privacy regulators in other jurisdictions are cooperating to ensure age assurance is implemented in a privacy-preserving manner.

Many of the reform proposals from the Privacy Act review – including increased transparency and accountability requirements, as well as increased rights to redress for individuals – reflect

[626] Privacy Act Review – Report, Proposal 16.2.
[627] Privacy Act Review – Report, Proposal 16.1 defines a child as an individual who has not reached 18 years of age.
[628] AGD, '*Online Privacy Bill Exposure Draft: Response 313221004*', AGD website, 2021, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?uuId=313221004.
[629] Privacy Act Review – Report, Proposal 16.2.

feedback received through eSafety's consultations and could have implications for the application of certain age assurance technologies. It is important that any age assurance technologies which collect, handle, store or share personal information, are required to adequately protect Australians personal information thorough privacy legislation which requires them to:

- Take a data minimisation approach
- Notify individuals and the regulator of data breaches
- Be subject to investigation and appropriate penalties for breach of the legislation.

Senate Standing Committee on Economics Inquiry into the influence of international digital platforms

Related to this review, the Senate Standing Committee on Economics is conducting an Inquiry into the influence of large international digital platforms. [630] Part of this Inquiry is examining the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses.[631] It also covers related issues pertaining to children's safety and privacy. eSafety provided a submission to this Inquiry in February 2023 and is monitoring any further developments which may be of relevance to this report.

[630] Parliament of Australia, '*Influence of international digital platforms',* Parliament of Australia website, 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digitalplatforms.
[631] Influence of international digital platforms, 2022.

Security

Like privacy, security was raised as a critical issue in our consultations. Many of the frameworks discussed earlier in this chapter – including the TDIF and relevant international standards – have security requirements embedded within them, such as the use of modern security technology. This includes two-factor authentication, end-to-end encryption, and limiting the collection, use, storage and sharing of user data. Following the Inquiry, the Committee recommended the DTA, in consultation with the Australian Cyber Security Centre (ACSC), develop standards for online age verification.[632] Since then, as highlighted above, there has been ongoing work on relevant international standards, as well as significant progress on Australia's Digital Identity System. As a result, it is unclear at this stage whether further standards may be needed, or whether, in accordance with Enex TestLab's assessment, more specific assessment frameworks should be developed to support benchmarking against existing standards. eSafety suggests the ACSC, as the Australian Government's lead agency on cyber security, remain involved in further discussions and actions flowing from this report, including any pilot initiative. It is crucial that any age assurance or verification regime should reflect the goals and principles of the Australian Government's broader cyber and identity security agenda.

2023-2030 Australian Cyber Security Strategy

On 8 December 2022, the Minister for Cyber Security, the Hon. Clare O'Neil MP, announced the development of the 2023-2030 Australian Cyber Security Strategy (the Strategy).[633] The Minister has appointed an Expert Advisory Board to advise on the development of the Strategy.[634] As of March 2023, the Expert Advisory Board is currently consulting on a discussion paper on how the Australian Government can achieve its vision under the Strategy. While the paper does not contain specific references to age assurance, one of the potential action areas is designing and sustaining security in new technologies. eSafety will continue to engage with the ACSC to ensure developments in the Strategy consider, and are reflected in, any technological outcomes of the roadmap. Should the government support eSafety's recommendation to carry out a pilot, we suggest the pilot should involve ACSC and the Department of Home Affairs (DHA).

[632] House of Representatives Standing Committee on Social Policy and Legal Affairs, *Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*, 2020.

[633] Department of Home Affairs, '*2023-2030 Australian Cyber Security Strategy discussion paper*', 2022, available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper.

[634] Department of Home Affairs, *'2023-2030 Australian Cyber Security Strategy expert advisory board'*, available at: https://minister.homeaffairs.gov.au/ClareONeil/Pages/expert-advisory-board-appointed-as-development.aspx

Human rights

As set out in chapter 5, measures to restrict children's access to online pornography, including the use of age assurance and other online safety technologies, have human rights implications for both children and adults. These include the benefits to children's safety, making sure their best interests are reflected, and potential risks to privacy and freedom of expression. There are multiple initiatives underway within Australia to put strong human rights safeguards in place and promote the fair and equitable use of technologies, including those that rely on biometrics. In addition, the introduction of any digital identity legislation will need to be accompanied by a Statement of Compatibility with Human Rights.[635]

Proposed Human Rights Act

The Australian Human Rights Commission (AHRC) has advocated for the promotion and protection of human rights in the online environment, including for freedom of expression, privacy, and non-discrimination. It has produced several guidelines and resources to help individuals understand their rights and obligations when using online platforms.[636]

In December 2022, the AHRC published a proposed model for a national Human Rights Act to enshrine individuals' rights to the protection of children, privacy, freedom of expression, and liberty and security, among other rights.[637] Under a Human Rights Act, individuals could continue to make complaints to the AHRC about human rights breaches but there would also be a new pathway to bring claims before the courts. Should the government support eSafety's recommendation to carry out a pilot, we suggest the pilot should involve the AHRC, to ensure human rights requirements are appropriately considered.

Biometrics and human rights

Some stakeholders raised specific human rights issues with the use of biometrics for age assurance purposes. These included the privacy and security of sensitive information and concerns about the accuracy and potential discrimination if technologies have a higher error rate for some groups than others depending on factors such as gender, race, ethnicity and disability. The widespread use of biometric technologies also assumes individuals fully understand the implications of using the technology and give their informed consent before their data is collected, stored and processed. Stakeholders identified the need to not make

[635] AGD, *'Statements of Compatibility',* AGD website, n.d., https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/statements-compatibility.

[636] Australian Human Rights Commission, '*Human rights and the Internet*', AHRC website, 2013, https://humanrights.gov.au/our-work/rights-and-freedoms/projects/human-rights-and-internet.

[637] Australian Human Rights Commission, '*Position paper: A Human Rights Act for Australia*' - p18, AHRC website, 2022, https://humanrights.gov.au/human-rights-act-for-australia?mc_cid=ac070de646&mc_eid=17643dd35e.

these assumptions and always provide clear information about the technology, its purpose, and the potential risks and benefits.

Ongoing consideration of facial recognition technology and biometrics

AGD's Privacy Act Review report considered the risks posed by facial recognition and other biometric technology in the context of privacy. The report included discussion of the University of Technology Sydney's Human Technology Institute (HTI) report proposing a model law for facial recognition technology in Australia, released in September 2022.[638] The Institute consulted with an Expert Reference Group, which included members from the Department of Home Affairs.

Under HTI's proposed model law, anyone who develops or deploys a facial recognition technology application must first assess the level of risk to a user's human rights through a 'Facial Recognition Impact Assessment' (FRIA). This includes an assessment of how the technology functions, where and how it is deployed, the performance or accuracy of the application, the effect of any decisions made in reliance on the application's outputs, and whether affected individuals can provide free and informed consent. The FRIA process would assign a risk rating to the relevant technology: base-level, elevated or high risk. Assessments would be registered with a relevant regulator and made publicly available to ensure transparency of operation and use.

HTI's model law could also apply and extend existing privacy law obligations for facial recognition technologies and could provide for the creation of an enforceable facial recognition technical standard. Any further developments in relation to the regulation of biometrics should feed into any age assurance pilot. While the Privacy Act Review Report recommended that privacy impact assessments should be required for all high-risk practices, the Report also noted there may be merit in adopting the enhanced risk assessment process set out in the HTI's proposed model law given the special nature of face data and the particular risks posed by facial recognition technology. Future work will be undertaken to consider the HTI's proposed model law in further detail and determine the extent to which it could be accommodated into the Privacy Act framework.

[638] UTS Human Technology Institute, '*Facial recognition technology: Towards a model law*', 2022, https://www.uts.edu.au/sites/default/files/2022-09/Facial recognition model law report.pdf.

HTI's report proposes four key steps towards reform:

- The introduction of a bill into the Australian Parliament based on HTI's model law.
- The appointment of an independent regulator to create a facial recognition standard and provide advice to industry and the public.
- Commonwealth agencies should coordinate with state and territory counterparts to ensure the law is harmonised across all jurisdictions.
- The Australian Government should establish a dedicated taskforce on facial recognition technology to work with Commonwealth agencies to make sure the facial recognition technology meets legal and ethical standards, and to coordinate international efforts.

Consumer rights and competition

Individuals and businesses active in Australia are required to comply with competition, fair trading and consumer protection laws, in particular the Competition and Consumer Act 2010 (Cth) administered and enforced by the ACCC, and the Australian Consumer law, which is jointly administered and enforced by the ACCC and State and Territory consumer protection agencies.

One of the potential challenges of mandating age assurance technologies is making sure regulation does not stifle innovation and competition, particularly in growing sectors or markets prone to 'tipping', where one or two firms are left to dominate a market, potentially irreversibly.

In consultations, stakeholders raised the risk of entrenching and extending the dominance of first movers or large companies to the detriment of smaller businesses. Stakeholders also highlighted the cost of complying with age assurance measures for small businesses which offer access to online pornography. They pointed out that the costs of age assurance software or licensing third-party solutions from providers may be prohibitive for small businesses, depending on fee structures. As highlighted in chapter 5, they also emphasised that such options may not be proportionate to the risks smaller sites present to children – particularly those which are paywalled and have other protections in place.

Some stakeholders also questioned whether larger companies within the online industry may be purposefully undermining third-party safety technology providers – either to protect or promote their own competing safety tools, or because they have taken a particular policy stance on the appropriate balance between privacy and safety, which may be influenced by related business interests. Stakeholders called for greater transparency and consistency in the decision-making of these larger companies regarding user safety tools and controls, as well as greater choice in and control over safety tools for consumers, particularly parents.

Since 2020, the ACCC has been conducting an Inquiry into markets for the supply of digital platform services, with a series of interim reports delivered every six months from September 2020 to March 2025.[639] The second interim report, released in April 2021, considered competition and consumer protection issues associated with app marketplaces in Australia.[640] The report found the Google Play Store and the Apple App Store had market power in mobile app distribution in Australia, and it was likely this market power was significant. In the fifth interim report, provided to the Treasurer in September 2022, the ACCC recommended several measures that could be taken to address the competition concerns and the consumer concerns identified.

The sixth interim report, provided to the Treasurer in March 2023, considered competition and consumer issues in the provision of social media services to consumers and businesses in Australia.[641] Consistent with the findings of this eSafety report, some submissions to the ACCC pointed to the need for more robust age assurance processes to be carried out on social media services to create safe and age-appropriate experiences for younger users.[642]

Should the government support eSafety's recommendation to carry out a pilot, we suggest as part of the scoping process, consideration should be given to how an age assurance system could be set up in a way that does not create significant barriers to entry and expansion for smaller businesses, and which may foster, or at least not impede, innovation, competition and consumer choice. This could also be informed by DTA's work to develop a fair and transparent charging framework for the expansion of the Digital Identity System.[643] We also suggest the ACCC should be involved in this work, given its key role in protecting competition and consumer rights.

[639] Australian Competition and Consumer Commission (ACCC), '*Digital platform services Inquiry 2020-25*', ACCC website, 2020, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25.

[640] ACCC, *'Digital platform services Inquiry: March 2021 interim report',* ACCC website, 2021, https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-march-2021-interim-report.

[641] ACCC, *'Digital platform services Inquiry: March 2023 interim report',* ACCC website, 2021, https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/march-2023-interim-report.

[642] ACCC, '*Submissions to the issues paper*', 2022, https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25/march-2023-interim-report#:~:text=Submissions%20to%20the%20issues%20paper.

[643] DTA, '*Digital Identity legislation: what is it?*', Digital Identity System website, n.d., https://www.digitalidentity.gov.au/sites/default/files/2022-06/Digital Identity Legislation - what is it - overview factsheet_FINAL_revised 1 June 2022_1.pdf

Conclusion

In our consultations, stakeholders emphasised that any mandatory age verification regime should be underpinned by 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 in Australia that has the full breadth of experience and capability to deliver on all necessary functions.

However, this chapter canvasses the overall age and identity verification landscape in Australia, including the substantial work underway by the DTA to develop a regulatory scheme for Australia's Digital Identity System, the recent independent review of myGov and collaboration across states and territories, and the Data and Digital Ministers Meeting.

In addition, the AGD's Privacy Act Review report outlines proposals designed to ensure Australia's privacy framework is more responsive to the digital environment. This work, alongside relevant international standards, provide a basis for a regulatory accreditation and oversight system for age assurance. Further work to establish a suitable regulatory accreditation and oversight system could take place alongside the development and execution of an age assurance pilot. This would increase Australia's readiness to implement any age assurance or verification regime, should the pilot prove successful.

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 are interwoven across multiple departments and portfolios. It is crucial that government is operating in a collaborative and streamlined manner on the development and evaluation of any pilot stemming from the roadmap, as well as the implementation of any ongoing age assurance policy or regime. As highlighted in this chapter, eSafety suggests an effective approach to cross-government efforts would include digital investment oversight and strategic policy leadership provided by the DTA, supported by the other departments and agencies identified in this chapter.

Chapter 10: International developments on age assurance and restricting children's access to online pornography

Key points:

- Countries are at various stages of considering, implementing or enforcing such measures, however the international legal landscape is rapidly changing. There is increasing support for introducing measures that identify child users and protect their safety and privacy.
- At a national-level approaches differ, including the extent to which age assurance technologies are prescribed. However, there are common principles shared by several jurisdictions, including proportionality, accuracy, transparency, security, compliance with laws, data minimisation and privacy protection.
- International law requirements and their application varies by the type of online service. In the EU, the Audiovisual Media Services Directive and the new Digital Services Act provide some baseline consistency. In addition, many countries (including Australia) have drawn inspiration from the UK's Age-Appropriate Design Code for safeguarding children's data.
- Media regulators in some countries are working with privacy regulators on joint solutions, acknowledging the importance of data and privacy protection online.
- Common complementary measures to prevent harm to children from pornography include providing education, requiring inbuilt safety measures (e.g., default filters and controls) and implementing protection measures through mobile phone companies and device manufacturers.
- Countries which have passed relevant laws face enforcement challenges, highlighting the importance of international collaboration and coordination.

Overview

This chapter explores international legislative, regulatory, and technical developments in relation to children's access to online pornography. It provides an overview of policy and legislation in countries that have been most active in considering or implementing age assurance and related measures, including Germany, Cyprus, the United Kingdom, France, the United States, the Republic of Korea, Japan, the Philippines and Canada.

Globally, education is recognised as an important lever for mitigating the risk of harm to children from accessing online pornography. Domestic and international educational approaches are covered in Chapter 13.

While this chapter touches on technical interventions adopted by international jurisdictions, detailed discussion of international standards for age assurance technologies and related developments are in Chapter 9.

During consultations, stakeholders emphasised the importance of an internationally collaborative approach to the regulation of online services, especially as many online services which host pornographic content operate across national borders. They consistently raised the importance of harmonisation and interoperability to increase effectiveness, to reduce cost and regulatory burden, and to mitigate the risk of fragmentation. Stakeholders noted that having vastly different approaches across different countries creates opportunities for online service providers and users to circumvent jurisdiction-based restrictions. For example, providers can move operations to a different location and users can turn on a Virtual Private Network (VPN) to access geo-blocked content. Conversely, a coordinated approach is likely to reduce evasion, increase compliance and ultimately enhance children's safety by working towards a global standard.

Accordingly, to develop this report eSafety engaged overseas counterparts, including members of the EU age verification working group, to understand jurisdictional arrangements, successes and challenges. eSafety has also maintained a watching brief on international developments in: research, educational initiatives, technological assessments, policy discussions, legislative and regulatory proposals and approaches, enforcement activities, and reforms relating to age assurance requirements and complementary safety measures. We seek to draw on their experiences to inform Australia's approach.

International developments by jurisdiction

Europe-wide legislation

Audiovisual Media Services Directive

The European Parliament adopted the European Union (EU) Audiovisual Media Services Directive (AVMSD) in October 2018.[644] The AVMSD governs EU-wide coordination of national legislation on all audiovisual media, including video-sharing platforms. It has multiple objectives, including creating a level playing field for emerging audiovisual media, protecting children and consumers, and guaranteeing the independence of national media regulators.

Under the AVMSD, video-sharing platforms must protect children from audio-visual content which may 'impair their physical, mental or moral development'.[645] Each EU Member State must appoint a regulatory body to determine which measures are appropriate to meet these rules, including age verification measures, and then bring these measures into their national law.

Under the AVMSD's country of origin principle, service providers must only abide by the rules incorporated into the law of the single EU Member State where their central administration is located, and not all Member States.

Digital Services Act

In November 2022, the Digital Services Act (DSA) came into force. Designed as a single, uniform set of rules for the EU, the DSA creates new obligations for online platforms to reduce harms and counter risks online, introduces strong protections for users' rights, and places digital platforms under a new transparency and accountability framework.[646]

Under the DSA, 'very large online platforms' – defined as companies which individually reach more than 10% of the EU population, or about 45 million people – will have to undertake a comprehensive assessment of risks to fundamental rights, including the rights of the child.[647] The EU Commission has the power to directly supervise these platforms.

As of February 2023, 18 platforms and search engines have self-reported having over 45 million EU users. Pornhub has estimated it has 33 million average monthly EU users, calculated as an average over the period of the past six months.[648] Meeting the threshold for very large online

[644] European Parliament, '*The Audiovisual Media Services Directive Briefing*', European Parliament website, 2019, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2016)583859.

[645] Official Journal of the European Union, '*AVMSD Directive (EU) 2018/1808*: *Article 28b*', 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN

[646] European Commission, '*Press Release - Digital Services Act: EU's landmark rules for online platforms enter into force*', European Commission website, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6906.

[647] Press Release - Digital Services Act: EU's landmark rules for online platforms enter into force, 2022.

[648] Pornhub, '*Pornhub submission: EU Digital Services Act*', Pornhub website, n.d., https://www.pornhub.com/information/eu_dsa.

platforms is likely to have a significant impact on pornography sites' obligations to prevent access by children.

Germany

Legislation

Germany's *Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in the Media* (JMStV) came into force in 2003,[649] making it the longest-standing legislation to be considered in this report.

The JMStV regulates all electronic information and communication media and broadcasting services. It was amended in 2020 to reflect the changing digital landscape, including video-sharing services.[650]

Its objective is to protect children and adolescents against electronic information and communication media which harms their development or education, and content which violates human dignity or other legal goods protected under the German Criminal Code.[651]

Providers of content that may 'impair the development of children or adolescents into self-responsible and socially competent personalities' must make sure young people do not access this content.[652] The distribution of pornography through media or teleservices is prohibited unless the provider ensures the material is only made accessible to adults.[653] Providers can fulfill this obligation by making it impossible or very difficult for children or adolescents to access this content through 'technical or other measures', or by situating the content behind software which identifies content that is unsuitable for a particular age group.[654] In effect, age verification is mandatory for all sites and online services that provide access to pornography.

[649] Kommission für Jugendmedienschutz (KJM), '*11th (2010) Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia: Section 1, Article 5 and Section 3, Article 11*', 2010, https://www.kjm-online.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Interstate_Treaty_on_the_Protection_of_Minors_in_the_Media__JMStV_in_English___13th_Interstate_Broadcasting_Treaty.pdf.

[650] Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM), '*Legal Foundations Germany*', FSM website, n.d., https://www.fsm.de/en/knowledge/

[651] KJM, '19th (2016) Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia', Section 1, Article 1, KJM website, 2016, https://www.kjm-online.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Interstate_Treaty_on_the_Protection_of_Minors_in_the_Media__JMStV_in_English___19th_Interstate_Broadcasting_Treaty.pdf.

[652] KJM, 11th (2010) Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia, Section 1, Article 5(1), KJM website, 2010.

[653] KJM, 19th (2016) Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia, Section 1, Article 4(2). Note this does not include 'hard pornography' defined separately in the Act, which is illegal without exception.

[654] KJM, 19th Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia, Section 3, Article 11.

Authorities

Under the JMStV, Germany's 14 state media authorities are responsible for the protection of minors in 'telemedia'. Telemedia is defined as electronic information and communication services including websites and other online offers of goods and services, video-on-demand platforms and advertising emails.[655] As broadcasting regulations are state matters under the German Constitution, state media authorities regulate private broadcasting and are independent of the State. Their work includes media literacy which has led to the development of platforms like Internet ABC, Klicksafe and Flimmo, which aim to help young people develop online competencies, and enable parents, carers and educators to make age-appropriate choices.

The Kommission für Jugendmedienschutz (Commission for the Protection of Minors in the Media, or KJM) is the central supervisory authority for youth protection in private broadcasting and telemedia. The KJM evaluates potential breaches of JMStV provisions and determines consequences for relevant providers.

Accreditation of age verification products

KJM indicates that age verification should occur through a two-step process[656]:

- a one-time validation of personal identity including verification of age.
- authentication during use to make sure only the identified and age-verified person has access to content.

KJM has developed and published process-based criteria to evaluate age assurance technologies.[657] These criteria include:

- whether the technology verifies age with a high degree of certainty. Where service providers choose to adopt age estimation mechanisms, they are required to implement a buffer of five years to combat the risk of underage access. When this requirement is applied, a person aged 18 must be estimated at 23 years to access online pornography.
- whether user data is recorded and stored in compliance with data protection regulations.
- the availability of a registration point where all personal data relevant to the age verification is collected and forwarded to the age verification service provider.

[655] D Klein, Telecommunications-Telemedia Data Protection Act (TTDSG) - Summary of the main provisions, Taylor Wessing website, 2022

[656] KJM, Age verification systems, KJM website, n.d., https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/.

[657] KJM, Age verification systems.

When products successfully meet these criteria, they are added to a list of approved age verification technologies.658 This is done to help online service providers meet their obligations and to ensure transparent decision-making processes and development of standards.[659]

As Germany requires telemedia to undertake age verification prior to providing access to adult content, age estimation technologies are only approved as a partial solution to be used in conjunction with other forms of assurance. The categories of age assurance technologies approved by KJM and some examples of each are provided below:

Account-based authentication	Hard identifiers	Age estimation – biometric	Age estimation - AI
• Sofort Ident+ by Sofort GMBH • Pay N Play' of Trustly Group AB • AdultPark by Arcor AG & Co. KG	• Checkin.com ID Scan by Checkin.com Group • Nect Ident • IDnow Digital Identity Wallet by IDnow GmbH	• Yoti Age Scan by Yoti Ltd • Facial age estimation by KYC AVC UK Ltd	• Ageware by Biometric Ventures s.r.o. • Face Assure by Privately SA

Compliance and enforcement

German regulators can enforce the JMStV by requiring other service providers, such as web hosting companies and internet service providers, to block German users' access to noncompliant services.[660] Providers that violate their obligations may be imprisoned or fined up to €300,000.[661]

When the JMStV took effect, some pornography sites that had been based in Germany decided to relocate to other jurisdictions. Others, such as Fundorado.de and Veegaz.com, chose to stay in Germany and implement the age verification requirements. Importantly, these sites have been able to achieve compliance while also maintaining successful business operations. While this demonstrates that compliance is achievable, it has not been widespread. Between March and June 2020, the North-Rhine Westphalia Media Authority contacted the providers of four major pornography websites which were accessible from Germany but had not implemented

[658] KJM, Age verification systems.
[659] KJM, Age verification systems.
[660] Simmons & Simmons, The new German State Media Treaty - legal requirements on telemedia, Simmons & Simmons website, 2020, https://www.simmons-simmons.com/en/publications/ckdhmlhufqy9g09265hhz6tw1/the-new-german-state-media-treaty---legal-requirements-on-telemedia.
[661] KJM, 19th Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia, Articles 23 & 24.

any form of age verification: Xhamster, owned by Hammy Media, and YouPorn, Pornhub and MyDirtyHobby, owned by MindGeek.[662]

MindGeek declined to implement age verification on some of its sites and a blocking order was issued. Mindgeek applied to the court for legal protection on the basis it was not within Germany's jurisdiction (Pornhub has subsequently notified they are based in Cyprus). In November 2021 and subsequently in September 2022, the relevant Administrative and Higher Courts upheld the blocking order, holding that the JMStV applies to sites operating outside of Germany and that protection of online services is less important than the protection of children.[663] However, as of February 2023, blocking had not yet been instituted.

Hammy Media did not respond to the regulator's outreach, nor did its Netherlands-based hosting service provider. A blocking order was therefore issued in relation to Xhamster.com. This order was in force for one day before a 'mirror' site with the same content emerged at Xhamster.de. Currently, there is no expedited process to require blocking of mirror sites and the requisite court process was re-initiated.

While non-compliant providers can be fined, Germany cannot enforce a fine against an internationally-based pornography site for violating the JMStV. Additionally, there are no powers to require payment providers facilitating the operation of these sites to cease providing support. These are important factors for Australia to consider as it contemplates how age verification requirements may be designed, implemented and enforced.

Cyprus

Authority

The Cyprus Radio Television Authority (CRTA) was established in 1998 under the Radio and Television Stations Law 7(I)/1998.[664] It regulates the establishment, installation and operation of private radio and television stations in the Republic of Cyprus. The CRTA is currently drafting regulations to transpose the AVMSD into the Radio and Television Stations Law 7)(I)/1998.

Legislation, platforms and concerns

Article 32(E)(7) of the transposed AVMSD imposes notification requirements on new and existing video-sharing platform providers based in Cyprus. Existing providers were required to inform CRTA within one month of the law coming into force. As part of this process, five video-

[662] M Burgess, '*Germany is about to block one of the world's biggest porn sites*', Wired, 2021, https://www.wired.co.uk/article/germany-porn-laws-age-checks.
[663] S Klein, '*[DE] Cypriot pornographic website ban confirmed*', IRIS Merlin website, 2022; Associated Press Berlin, German court OKs ban on Cyprus-based porn sites, Spectrum News 1, 2021, https://merlin.obs.coe.int/article/9584.
[664] Mediterranean Network of Regulatory Authorities (translated), '*CRTA (Cyprus Radio Television Authority)*', Mediterranean Network of Regulatory Authorities website, n.d., https://www.rirm.org/en/crta-cyprus-radio-television-authority-2/.

sharing platforms submitted notification forms as of January 2023 (Stripchat, Xhamster, Pornhub, Fabhouse and Virtual Taboo). Fabhouse denied it fell within the definition of a video-sharing platform.

Platforms raised concerns about the incoming regulations, including unfair competition from non-EU based companies, the cost-effectiveness of age verification, and data privacy and security. CRTA is working through these issues in discussion with platforms, civil society and the public.

Privacy and data protection

The CRTA has also worked with the Cypriot Commissioner for Personal Data Protection on age verification. Discussions about age verification mechanisms and related privacy risks are ongoing. However, the Commissioner and CRTA have agreed that video-sharing platforms need advance approval from the Commissioner before using facial recognition methods, and storage of biometric data in any form will not be acceptable.

Collaboration between online safety and privacy regulators is a common theme of this chapter. Within Australia, eSafety works closely with the Office of the Australian Information Commissioner to promote a coordinated approach that balances safety and privacy considerations.

United Kingdom

Digital Economy Act

In 2017, the United Kingdom (UK) passed the Digital Economy Act (the DE Act), covering a broad range of subjects relating to electronic communications infrastructure and services. Part 3 of the DE Act included age verification for online pornography.[665] Under Part 3, websites that publish pornography on a commercial basis would have been required to implement a 'robust' age verification system. The British Board of Film Classification (BBFC) was charged with enforcing this legislation. However, in October 2019, the UK's Secretary of State announced the government would not be proceeding with Part 3 and that age verification objectives would be delivered through the proposed online harms regulatory regime instead.[666]

[665] UK Legislation, '*Digital Economy Act 2017: Part 3 online pornography*', legislation.gov.uk website, 2017, https://www.legislation.gov.uk/ukpga/2017/30/part/3/enacted.

[666] N Morgan, '*Statement on online harms*', UK Parliament website, 2019, https://questions-statements.parliament.uk/written-statements/detail/2019-10-16/HCWS13.

AVMS Regulations

When the UK formally left the EU in 2020, it transposed the AVMSD into Part 4B of the *Communications Act 2003*.[667] In November 2020, the Audiovisual Media Services (AVMS) Regulations gave the UK Office of Communications (Ofcom) powers to regulate UK-established video-sharing platforms.[668]

In the UK Communications Act, video-sharing platforms are defined as services whose principal purpose or essential functionality is provision of videos to members of the public.[669] These platforms operate through an electronic communications network, on a commercial basis, and in such a way that the service provider does not have general control over what videos are available on it but controls how videos are organised. These platforms also include services that enable users to upload videos and engage with other users' content and livestreams. Examples of services covered under this definition include Snapchat, OnlyFans, TikTok, Twitch and Vimeo.[670] Platforms that may be covered in the future could include some of the most popular online pornography services in the UK, such as PornHub, Redtube and YouPorn, which fall under this definition.

Video-sharing platforms generally exclude services allowing users to upload and share videos within a business intranet; online newspapers where videos are embedded within the journalistic or editorial content; television interfaces that provide access to a third-party platform, on-demand programme services[671] and linear services; video-conferencing technologies facilitating private video calls; and 'on-demand' or 'catch-up services' that broadcast on a television channel's own website.[672]

Ofcom's guidance to comply with the AVMS Regulations states that if a video-sharing platform 'has restricted material on its service that is of a pornographic nature, providers should have a robust access control system that verifies age and prevents under-18s from accessing such material.'[673] The regulatory guidance clarifies that age verification measures should either act as an age-gate that blocks access to the entire platform or filters content in a way that protects minors. The guidance also encourages providers to conduct a risk assessment of their platform,

[667] UK Legislation, '*No. 1062 BROADCASTING: The Audiovisual Media Services Regulations 2020',* legislation.gov.uk website, 2020, https://www.legislation.gov.uk/uksi/2020/1062/made/data.pdf.

[668] Ofcom, '*Guidance: Video-sharing platforms – who needs to notify to Ofcom?*', Ofcom website, 2021, https://www.ofcom.org.uk/online-safety/information-for-industry/vsp-regulation/guidance-who-to-notify-to-ofcom.

[669] UK Legislation, *'Communications Act 2003*', Part 4b 368S, legislation.gov.uk website, 2003, https://www.legislation.gov.uk/ukpga/2003/21/part/4B.

[670] Ofcom, '*Notified video-sharing platforms*', Ofcom website, 2023, https://www.ofcom.org.uk/online-safety/information-for-industry/vsp-regulation/notified-video-sharing-platforms.

[671] Defined as providers that have control over what videos are available on their service.

[672] Ofcom, *'Video-sharing platforms: who needs to notify to Ofcom? Guidance notes',* p8 para3.8, Ofcom website, 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0023/215456/guidance-video-sharing-platforms-who-needs-to-notify.pdf.

[673] Ofcom, *'Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material',* para4.94, Ofcom website, 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0023/215456/guidance-video-sharing-platforms-who-needs-to-notify.pdf.

accounting for the risk of harm posed to children by the type of restricted material on the platform and the prevalence of such material.[674]

The guidance suggests platforms also consider:[675]

- assessment of who is using the service (in a privacy-preserving manner)
- consideration of reliability and accuracy of any age assurance method and the level of confidence it provides against the risk
- easy integration of age assurance measures into platforms to preserve user experience, as this is likely to facilitate wide adoption and be sustainable
- adoption of design features which disincentivise circumvention, for example, not providing another chance to sign in once an underage age declaration is made.
- use of third-party age assurance service providers which meet the requirements under PAS 1296 (discussed in chapter 9) and the UK's Digital Identity and Attributes Trust Framework or other relevant standards
- consideration of potential exclusionary risks to children.

These elements are useful when considering future Australian approaches.

Ofcom's guidance applies to video-sharing platforms specialising in pornography, as well as services that have a high prevalence of pornography. Unlike KJM in Germany, Ofcom does not suggest or endorse specific technological tools or methods platforms should implement, but rather requires that measure(s) are effective in preventing access to that material for children aged under 18. Ofcom also expects platforms to undertake ongoing assessment of emerging technologies for online safety.[676]

In October 2022, Ofcom released findings from its first year of video-sharing platform regulation, which included reports on Tiktok, Snapchat, Twitch, Vimeo, BitChute, OnlyFans and smaller adult platforms such as Admire Me, Fanzworld, Pocket Stars, RevealME and Xpanded.[677] In this report, Ofcom highlighted that OnlyFans has adopted age verification for all new UK subscribers in compliance with the new regulatory requirements.[678] Now, new subscribers are directed to third-party age estimation service provider Yoti to undertake facial estimation. If this fails, the subscriber is redirected to age verification app Ondato where they can upload a copy of their government ID before being able to access content on the app.

[674] Ofcom, Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material, para4.90.

[675] Ofcom, Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material, para4.108.

[676] Ofcom, '*Ofcom's first year of video-sharing platform regulation*', p101, Ofcom website, 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0032/245579/2022-vsp-report.pdf.

[677] Ofcom, Ofcom's first year of video-sharing platform regulation, p28.

[678] Ofcom, Ofcom's first year of video-sharing platform regulation, p94.

Notably, OnlyFans has not as yet extended this age assurance requirement to subscribers in jurisdictions such as Australia (though there are measures in place for content creators to safeguard against child sexual exploitation and abuse).[679] eSafety has had preliminary engagement with OnlyFans and would welcome applying the lessons learned from its efforts to comply with UK regulations to benefit users globally – much like Tinder has done in the Japanese context (*see: Japan*). Ofcom found smaller adult platforms did not have robust measures to prevent children from accessing pornography.[680] Three small adult service providers closed the video-sharing sections of their sites after concluding they would not be able to comply with Ofcom's expectations for age verification.[681] Others continue to operate without any measures to prevent children's access.

Online Safety Bill

Following a public consultation process on the online harms white paper in 2019, the Online Safety Bill was first published in May 2021 and introduced in the House of Commons on 17 March 2022.[682] The Bill was considered by a Public Bill Committee over 17 sittings between 24 May and 28 June 2022 and underwent further examination over 13 sittings in June 2022. Since then, the Bill has been amended several times. Amendments include improved transparency about how providers treat harmful content and the introduction of new user empowerment tools for adults, so people would be able to control what content they might see online. The revised Bill was introduced in the House of Lords on 18 January 2023.[683]

If passed, the Bill will:

- introduce legal duties on about 25,000 companies which fall under the definition of 'user to user' or search services to protect children. This includes a duty for providers of online pornography to make sure children are not normally able to encounter such content.[684]
- require services to use age verification systems or methods that deliver the same level of protection.[685]
- empower Ofcom to fine non-compliant providers up to 10 per cent of their annual worldwide turnover or block their sites from being accessible in the UK. Senior executives

[679] OnlyFans, '*Privacy Policy*', OnlyFans website, 2020, https://onlyfans.com/privacy.
[680] Ofcom, Ofcom's first year of video-sharing platform regulation, p17.
[681] Ofcom, Ofcom's first year of video-sharing platform regulation, p111.
[682] UK Parliament, '*Online Safety Bill: Commons stages*', House of Commons Library, 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9579/#:~:text=Documents%20to%20download&text=The%20Online%20Safety%20Bill%20%5BBill,online%20while%20defending%20free%20expression%E2%80%9D.
[683] UK Parliament, Online Safety Bill: Commons stages, 2023.
[684] UK Parliament, '*Analysis of the Online Safety Bill*', House of Commons Library, 2022, https://researchbriefings.files.parliament.uk/documents/CBP-9506/CBP-9506.pdf (page 21).
[685] UK Government, '*Online Safety Bill: Supporting documents*, Gov.UK website, 2022, https://www.gov.uk/government/publications/online-safety-bill-supporting-documents.

of these websites could also be held criminally liable if they fail to cooperate with Ofcom.[686]

Ofcom and the Information Commissioner's Office

Like Cyprus, online safety and privacy regulators in the UK have come together to consider good practice approaches to age assurance. In November 2022, Ofcom and the Information Commissioner's Office (ICO) strengthened their existing partnership through a memorandum of understanding (MoU) on online safety and data protection.[687] The purpose of the MoU is to enable the parties to share information on video-sharing platform regulation and age assurance, which enhances their ability to exercise their respective functions.[688] The MoU stipulates each party will alert the other to any potential legal breaches discovered in the course of their duties. It also requires parties to communicate regularly to discuss matters of mutual interest and seek to work collaboratively to maximise coherence and promote compliance.

Age-Appropriate Design Code ('the Children's Code')

Under the UK's *Data Protection Act 2018*, the ICO issued a statutory code of practice setting standards for online services which are likely to be accessed by people under 18. This is the Age-Appropriate Design Code (Children's Code), which came into effect in September 2021.

The Children's Code applies to all 'information society services' available in the UK that are likely to be accessed by users under 18, including apps, messaging services and games. It contains 15 standards to make sure services comply with obligations to protect children's data online.[689] The ICO monitors compliance through audits and complaints.[690] In September 2022, the ICO found that TikTok may have failed to protect children's privacy when using the TikTok platform, with the potential of a £27 million fine.[691]

Section 3 of the Children's Code states that services should 'either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing or apply the standards in this code to all your users instead.' Like the AVMS Regulations, the Children's Code does not prescribe the methods services should use to establish age, or what level of certainty different methods should provide. However, it does

[686] UK Parliament, '*Online Safety Bill*', UK Parliament website, 2023, https://bills.parliament.uk/bills/3137

[687] Digital Regulation Cooperation Forum, '*Online safety and data protection*', ICO website, 2022.

[688] Information Commissioner's Office, *Memorandum of Understanding between the Information Commissioner and Ofcom clause 11*, Ofcom website, 2019, https://www.ofcom.org.uk/__data/assets/pdf_file/0027/165933/mou-ico-ofcom.pdf.

[689] Information Commissioner's Office, '*Introduction to the Age appropriate design code*', ICO website, n.d., https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/.

[690] N Lomas, '*UK now expects compliance with children's privacy design code*', TechCrunch website, 2021, https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/

[691] Information Commissioner's Office, '*ICO could impose multi-million pound fine on TikTok for failing to protect children's privacy*', ICO website, 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/.

outline several methods services may wish to consider, from self-declaration to third-party age verification services.[692] These methods are explored in chapter 8.

In October 2021, the Information Commissioner issued an opinion on age assurance measures for the Children's Code. The opinion provides further detail on the level of certainty that various age assurance solutions provide; which providers or types of solutions comply with data protection requirements; and how to collect the additional personal data required for age assurance while complying with data minimisation principles.[693]

These principles only apply to organisations which process data for age assurance purposes, as opposed to providers of age-restricted services. The principles and a brief explanation are below:

Lawfulness and Accountability: organisations must comply with relevant laws and be able to demonstrate how they comply with the law in their age assurance activities.

Fairness: processing of personal data must be fair and must not be processed in a way that is detrimental, misleading or discriminatory towards users.

Transparency: organisations need to be clear, open and honest about how they use personal data for age assurance purposes, and how they make decisions as a result.

Purpose limitation and data minimisation: organisations using age assurance must apply data minimisation to their chosen approach. Any data processed for age assurance purposes must be adequate, relevant and processed for a specific purpose, limited to what is necessary.

Accuracy: organisations must monitor and consider any challenges to the accuracy of data. Data subjects should have the right to correct any inaccuracies in their personal data.

Storage limitation: organisations must not keep any personal data for longer than it is needed.

Security: organisations must process personal data used for age assurance securely. If using artificial intelligence (AI) technology, organisations much consider the balance between transparency and security.

[692] Information Commissioner's Office, '*3. Age appropriate application*', ICO website, n.d., https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/.

[693] UK Information Commissioner's Office (ICO), '*Information Commissioner's opinion: Age assurance for the Children's Code*', 2021, available at: https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf.

For biometric age assurance measures (such as facial or voice analysis), the Commissioner's opinion includes further considerations:

Biometric data: technologies that process biometric data to uniquely identify an individual should comply with relevant legal requirements.

Statistical accuracy: organisations should make sure any automated decision-making system is sufficiently statistically accurate and avoids unjustifiable discrimination.

Algorithmic bias: Organisations should make sure algorithms are trained using high-quality and relevant data sets and consider the potential for bias in assessing biometric data.

Many of these principles are reflected in the stakeholder feedback eSafety received during consultations. eSafety has applied these principles in its analysis of age assurance technologies in chapter 8. The principles should be considered for future Australian approaches emerging from, or after, this report. Measures based on the Children's Code have been proposed in the United States, and more recently in Australia.

Network and Device Level Filtering

In the UK**,** major internet service providers (ISPs) provide customers network filters to block adult or illegal content. 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. However, when these controls were used, only 6% of children have circumvented them and only 5% used a proxy server to avoid them.[694]

Since the publication of the BBFC Mobile Classification Framework in 2013, mobile network providers have restricted access to commercial content unsuitable for people under the age of 18.[695] If a person wants to remove age-restricted content settings on their mobile phone, they are generally required to provide personal credit card details to their mobile service providers or visit a store with a form of government ID to prove they are over 18.[696]

Age Verification for Other Purposes

In 2022, the UK Home Office led nine trials of digital age verification technologies in supermarket checkouts. The trials enabled age assurance service providers to test innovative

[694] Ofcom, '*Children and parents: media use and attitudes report 2022*', Ofcom website, 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf.

[695] British Board of Film Classification, '*Mobile content classifications*', BBFC website, 2013, https://www.bbfc.co.uk/about-classification/mobile-content.

[696] For example, Vodaphone one of the largest mobile phone providers in the UK have their requirements outlined here which include user credit card details or in person verification of government-issued ID.

approaches to age verification, such as digital ID, in the context of the sale of alcohol. Key takeaways were as follows:[697]

- uptake of age estimation technology at self-scan checkouts indicated there is appetite for digital age assessment.
- most trials of digital ID apps experienced very low take up.
- although trials did not assess accuracy of the technology, they did demonstrate the technology is sensitive to several environmental factors that could impact reliability. This includes positioning of equipment relative to bright light.
- several trials aimed to explore whether technology could reduce queuing time to enter licensed premises. Findings were inconclusive and suggest speed of entry to venues is dependent on practical factors, such as phone battery and Wi-Fi signal strength.

Any age assurance trials in Australia should seek to build on the lessons learned from these and other global trials.

France

Age Verification Legislation

In France, Article 23 of *Act No. 2020-936 of 30 July 2020 to Protect Victims of Domestic Violence* requires online publishers to prevent those under the age of 18 from accessing online pornography.[698] The law applies to all providers of adult content online whose services are available in France.

The AVMSD has been transposed into French law by Ordinance no. 2020-1642 of 21 December 2020 transposing Directive 2018/1808 of the European Parliament; the Council of 14 November 2018 amending Directive 2019/13/EU aimed at the coordination of certain legislation; and law no. 86-1067 of September 30, 1986, relating to freedom of communication.[699]

If a provider is found to be allowing children to access online pornography, the French Regulatory Authority for Audiovisual and Digital Communications (Arcom) can send a notice ordering the provider to take all possible steps to prevent minors from accessing the content. The recipient has 15 days to respond. If they fail to deploy age verification measures, Arcom can apply for a court order for the site to be blocked. Decree No. 2021-1306 of 7 Oct 2021 sets out

[697] UK Government, '*Key learning from the trial of age verification technology in alcohol sales*', Gov.UK website, 2022, https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox/key-learning-from-the-trial#trialling-digital-technology.

[698] Legifrance, '*Authenticated Electronic Official Journal No. 0187*', Legifrance website, 2020, https://www.legifrance.gouv.fr/download/pdf?id=shLVial2GFAvXVHYawAie63PzXyh2U2x_naRfEud_Wg=

[699] euCONSENT, '*EU Member State Legal Framework*', euCONSENT website, 2021, https://euconsent.eu/download/eu-member-state-legal-framework/.

the requirements for Arcom in issuing the notices and assessing evidence received in response.[700]

Enforcement Action

In December 2021, Arcom derived notices from the Conseil supérieur de l'audiovisuel (CSA) and issued them to Pornhub, XnXX, Xvideos, Tukif and Xhamster, requesting they prove their compliance with Article 23. With no response, Arcom applied for court orders to block the sites at the ISP level.[701] Pornhub, Xvideos and Xnxx lodged an appeal with the Conseil d'État against the formal notices, which was subsequently rejected. As of February 2023, Arcom and Pornhub have completed a confidential court-ordered mediation process. Arcom is expected to once again request court orders to block these websites at the ISP-level in the coming months.

Separately, Xvideos and Xnxx lodged an appeal against the decree implementing the law, which could result in its annulation. Arcom is currently awaiting a decision by the Conseil d'État. While the proceedings are underway, these websites remain unblocked in France. However, if the courts decide these sites should no longer be accessible from France, anyone trying to access these websites from a French IP address will be automatically redirected to an information page explaining the reason for this blocking.[702]

Data Privacy and Age Verification

Unlike the German regulators, Arcom does not publish an approved list of age verification measures. However, the French data privacy regulator, Commission Nationale de l'Informatique et des Libertés (CNIL), provides analysis and advice on a range of age verification systems.[703] The CNIL calls for age verification measures to be structured around six pillars:

Data Minimisation: any system should be designed to limit the collection of personal data to what is strictly necessary for verification, and not retain data once the verification has been completed. The data should not be used for other purposes, including commercial uses.

Proportionality: online service providers should consider the purpose of processing, target audiences, type of data processed, technologies available and level of risk associated with the processing.

[700] A Blocman, '*[FR] Access for minors to pornographic websites: Arcom's powers stipulated by decree*', IRIS Merlin website, 2021, https://merlin.obs.coe.int/article/9342

[701] Arcom, '*Access of minors to pornographic sites: Referral to the President of the Paris Judicial Court*', Arcom website, 2022, https://www.arcom.fr/larcom/presse/acces-des-mineurs-aux-sites-pornographiques-saisine-du-president-du-tribunal-judiciaire-de-paris.

[702] Arcom, Access of minors to pornographic sites: Referral to the President of the Paris Judicial Court, Arcom website, 2022.

[703] CNIL, *'Online age verification: balancing privacy and the protection of minors',* CNIL website, 2022, https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

Robustness: age verification mechanisms should be more robust when they are in place to prevent high levels of risk to children. In these circumstances, self-declaration of age on its own is not sufficient.

Simplicity: providers should use simple and easy-to-use solutions. This might include mechanisms which combine verification of both age and parental consent.

Standardisation: industry standards and a certification programme should be encouraged to ensure compliance with these rules and to promote verification systems suitable for a wide range of online services.

Third-party intervention: the use of trusted third-party providers should be investigated to meet the requirements described above in a privacy-preserving way.[704]

Similar to ICO's principles under the Children's Code, these pillars are reflected in eSafety's consultations and analysis of age assurance technologies in chapter 8.

Digital Certification Project

Since July 2022, CNIl and Arcom have been collaborating with age verification service providers to provide an effective verification option which promotes both safety and privacy. This project involves trialling the use of identity exchange services and a double-blind approach to protect user data, based on the euCONSENT pilot (see: chapter 8). The double-blind approach refers to an arrangement where the proof of age provider generates an age-assured token, but the provider is not privy to where the token is being used. A pornography website can accept the age-assured token to permit access but is not privy to the identity of the token-holder.[705]

Under this project, the French government announced that people seeking to visit pornography sites will have to install an application for government-licensed digital certification on their mobile phones to prove they are at least 18 years old.[706] Although details have not been finalised, proof of age may also be undertaken by a mobile service provider, digital identity provider or other organisation. Failure to comply may result in fines of 1% of global turnover or a

[704] CNIL, '*Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy*', CNIL website, 2021, https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy.

[705] F Hersey, *'Double anonymity to bring age verification to porn and social media in France',* Biometric Update.com website, 2023, https://www.biometricupdate.com/202302/double-anonymity-to-bring-age-verification-to-porn-and-social-media-in-france#:~:text=The%20concept%20for%20double%20anonymity,know%20his%20or%20her%20identity.

[706] M Strauss, '*France moves to block access to pornography sites for minors'*, Reuters website, 2023, https://www.reuters.com/world/europe/france-moves-block-access-pornography-sites-minors-2023-02-06/.

ban from publishing in France.[707] It is expected that both Arcom and CNIL will be enforcing new legislation with technical guidance released soon.[708]

Although not mandatory, the French government is encouraging industry to trial this approach and some sites are already working on implementation. From eSafety's conversations with Arcom representatives, none are in effect as of February 2023.

Law no. 2022-300 Requiring Devices to Include Parental Controls

In March 2022, the French Government passed *Law no. 2022-300*. The law has been in effect since 5 September 2022 but is not yet fully operational. It requires all smartphone and internet-connected device manufacturers to install a parental control option on devices sold in France. Devices in scope are those sold with an operating system.[709] The parental control system must be provided at no additional cost and prompt activation on purchase.[710] The law prohibits data collection from such parental controls for commercial purposes.

A further decree will set out the technical specifications of such control systems and relevant enforcement measures, following public consultation and European Commission notification on 14 October 2022.[711] The implementing decree will also detail the means of monitoring the new legal scheme by the French National Frequency Agency, which may impose administrative fines up to €1,500 for an individual and up to €7,500 for legal entities for failure to comply within a specific period.[712] The law is expected to be published in April 2023 and come into effect in 2024.[713]

eSafety can regulate devices under industry codes or standards. eSafety will monitor developments in France regarding mandatory parental controls and consider these developments in relation to the second phase of industry codes development in Australia.

[707] L Kayali, '*No porn, no Instagram for kids: France doubles down on age verification*', Politico website, 2023, https://www.politico.eu/article/no-porn-no-instagram-for-kids-france-doubles-down-age-verification-emmanuel-macrons-nick-clegg/.
[708] F Hersey, Double anonymity to bring age verification to porn and social media in France, 2023.
[709] Osborne Clarke, '*Commission notified of France's mandatory parental controls on internet devices*', Osborne Clarke website, 2022, https://www.osborneclarke.com/insights/commission-notified-frances-mandatory-parental-controls-internet-devices.
[710] French Republic, *'Parental control required on internet-connected devices*', service-public.fr, 2022; Legifrance, LAW No. 2022-300 of March 2, 2022 to strengthen parental control over internet access means (1), Legifrance website, 2022, https://www.service-public.fr/particuliers/actualites/A15553.
[711] French Directorate-General for Enterprise, '*Results of the public consultation: parental control on internet access*', entreprises.gouv.fr, 2022, https://www.entreprises.gouv.fr/fr/consultations-publiques/resultats-de-la-consultation-publique-controle-parental-sur-acces-internet.
[712] Osborne Clarke, *'France makes parental controls mandatory on internet-connected devices',* 2022, https://www.osborneclarke.com/insights/france-makes-parental-controls-mandatory-internet-connected-devices.
[713] Osborne Clarke, France makes parental controls mandatory on internet-connected devices, 2022.

Information for Parents

The French Government also provides advice to parents on covering the matter of online pornography with their children and provides guidance on establishing safe internet settings and parental controls at home. This is discussed further in Chapter 13.

United States

California Age-Appropriate Design Code Act

The California Age-Appropriate Design Code Act (AADC Act) was signed into law in September 2022 and is modelled on the UK's Children's Code. It compels online services to proactively assess the privacy and protection of children in the design of any digital product or service they offer. Specifically, it requires online services likely to be accessed by children to limit their collection of children's data, use age-appropriate language to communicate privacy terms of service, and provide an obvious signal to the child their activity is being monitored by a parent or carer.

Utah Filtering Measures

The Governor of Utah signed off on House Bill 72 in March 2021. This requires filters for pornographic content on all smartphones and tablets sold and activated in Utah.[714] Going a step beyond France's new measures, the law would require producers to have filters for pornographic content activated by default, with the option for adult users to deactivate the settings using a passcode from the device manufacturer.[715] The device would have to notify the user that content was being filtered.[716] The feasibility of implementing such measures has been widely questioned and resulted in the inclusion of a provision that legislation would not take effect unless five other states enacted similar laws.[717]

Louisiana Age Verification Law

Act 440 came into force in Louisiana on 1 January 2023. This law requires websites to offer 'reasonable age verification methods' and provide civil remedies for damages against commercial entities that distribute 'material harmful to minors'[718]. It is limited to websites on

[714] S Eppolito, '*Utah governor signs divisive measure to require porn filters*', AP News website, 2021, https://apnews.com/article/utah-anti-porn-filter-phone-tablets-f8276e2f3e0d682bf7c317860acc2b3c.
[715] Utah State Legislature, '*H.B. 72 Device Filter Amendments*', Utah State Legislature website, 2021, https://le.utah.gov/~2021/bills/static/hb0072.html.
[716] A Robertson, '*Utah passed a law making iPhones filter porn — but only if other states pass one, too*', The Verge, 2021, https://www.theverge.com/2021/3/21/22335928/utah-phone-tablet-anti-porn-filter-law-passes-first-amendment.
[717] S Eppolito, Utah governor signs divisive measure to require porn filters, 2021.
[718] Louisiana State Legislature, *'Louisiana Revised Statutes of 1950, R.S. 9:2800.28, relative to material harmful to minors',* Louisiana State Legislature website, 2022, https://legis.la.gov/legis/ViewDocument.aspx?d=1289498.

which more than a third of the content falls within the definition of harmful material, meaning certain social media and online platforms may not meet this threshold.

'Material harmful to minors' is defined as material that the average person, applying contemporary community standards, would find is designed to appeal to 'prurient interest' or material that exploits, or is devoted to, actual, simulated, or animated display or depiction of the following, in a manner patently offensive with respect to minors:

- pubic hair, anus, vulva, genitals, or nipple of the female breast.
- touching, caressing, or fondling of nipples, breasts, buttocks, anuses, or genitals.
- sexual intercourse, masturbation, sodomy, bestiality, oral copulation, flagellation, excretory functions, exhibitions, or any other sexual act.

'Reasonable age verification methods' include verifying that the person seeking to access material is 18 years of age or older, by using a digitised identification card (as defined in R.S. 51:3211[719]). It can also include a commercial age verification system that relies on government-issued identification or transactional public or private data (such as mortgage, education, and employment information) to verify the person's age.

The law further states that identifying information, once access has been granted, should not be retained by the commercial entity or third party that performs the age verification process.

To date, reports have indicated that some websites (such as Pornhub and its intermediaries) are directing Louisiana-based users to AllPassTrust, a third-party identity verification site connected to LAWallet[720], Louisiana's digital driver's license.[721]

Concerns have been raised about the viability of the law due to interstate commerce and privacy concerns[722] as well as reports that using a VPN allows users in Louisiana to bypass the restrictions.[723]

[719] Louisiana State Legislature, *'Louisiana Revised Statutes of 1950, R.S. 51:3211 and 3212, relative to the use of digitized identification cards'*, Louisiana State Legislature website, 2020, https://www.legis.la.gov/legis/ViewDocument.aspx?d=1189752.

[720] LA Wallet, '*Official Digital Driver's License App for the State of Louisiana',* LA Wallet website, 2016, https://lawallet.com/.

[721] S Cole, 'You Now Need a Government ID to Access Pornhub in Louisiana', Vice, 2023, https://www.vice.com/en/article/4axe8d/louisiana-is-making-it-harder-to-watch-porn.

[722] V Skinner, '*New Louisiana law on age verification for porn sites could face legal challenge*', The Center Square, 2023, https://www.thecentersquare.com/louisiana/new-louisiana-law-on-age-verification-for-porn-sites-could-face-legal-challenge/article_dd61170a-8dff-11ed-9535-af889ee1c000.html.

[723] M Eddy, '*Louisiana's New Porn Law Is a Privacy Time Bomb*', PC Mag website, 2023, https://au.pcmag.com/security/98095/louisianas-new-porn-law-is-a-privacy-time-bomb.

Republic of Korea ('Korea')

Identity Verification for Online Pornography

In Korea, online content is regulated through two bodies: the Korean Communications Committee (KCC) and the Korean Communication Standards Committee (KCSC). KCC is responsible for regulating all media content and publishers, while KCSC specifically regulates the Internet.

Korea adopted ID-based age verification in 2007, using a double-blind approach. The system asks users who visit any websites for the first time to verify their identity through various ways, such as resident registration number, credit card number, certification, and Internet Personal Identification Number (i-PIN)[724]. It is designed so websites do not store user identity information obtained during the identification process. Websites verify user identity through the user identity database that is controlled by organisations having legal mandates. Only the result of identity verification is stored.[725]

Pornographic websites (as well as gambling and North Korea-related websites) are blocked in Korea. A list of web addresses that host such content is maintained by KCSC, which mandates internet operators block access by monitoring the Server Name Identification field.[726] This approach has faced criticism for its broad definition of 'harmful' content and its potential for censoring internet usage.[727]

Digital Identity Verification for Other Age-Restricted Products

Since late 2022, Korea's residents have been able use a digital version of their national identity card on their mobile devices. This enables users to prove their age when purchasing age-restricted goods and to verify their identity when signing contracts and other legal documents.[728]

The 'Pass verification app' was launched in 2018 (by three Korea-based mobile network operators – SK Telecom, KT and LG U+) and previously enabled users to upload mobile driving

[724] Korea Communications Commission, '*Understanding Korea's 'Identity Verification System'*, Korean Government website, 2009, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjugdTro778AhVpwjgGHa22Bpo4ChAWegQICBAB&url=https%3A%2F%2Fwww.korea.kr%2Fcommon%2Fdownload.do%3FfileId%3D166805504%26tblKey%3DGMN&usg=AOvVaw1SIvPg__OX31saJ_PkJnnG

[725] Korea Communications Commission, Understanding Korea's 'Identity Verification System', p4.

[726] The Korea Bizwire, '*South Korea Bans Access to Porn Sites*', The Korea Bizwire website, 2019, http://koreabizwire.com/south-korea-bans-access-to-porn-sites/132882.

[727] D Volodzko, '*Is South Korea Sliding Toward Digital Dictatorship?',* Forbes website, 2019, https://www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/?sh=20837fec648e; R Garcia*, 'Internet Censorship is Part of South Korea's Democracy Package*', The New Lens website, 2019, https://international.thenewslens.com/article/122579.

[728] F Hersey, '*South Korea's digital identity blockchain prepares to add new credentials, go international*', Biometric Update.com, 2022, https://www.biometricupdate.com/202212/south-koreas-digital-identity-blockchain-prepares-to-add-new-credentials-go-international.

licences.[729] It has now been extended to incorporate support for digital national IDs. Once created in Pass, a user's digital ID card displays a QR code along with the name, date of birth and address registered on their resident registration card.[730] At this stage, the app can only be used for in-person verification and has not yet been enabled for online verification. Korea's Digital Government Agency is planning to launch a blockchain-enabled digital ID for Korean residents in 2024.[731]

Japan

Age Verification and Content Filtering for Online Pornography

The Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People came into force in 2009.[732] This law requires telecommunications operators providing internet services to users under 18 to limit their exposure to harmful content.[733] The definition of 'harmful content' includes material which induces young people to commit crimes, stimulates sexual desire, or contains atrocious descriptions of violence.[734]

Mobile phone companies, online services, social media platforms and dating apps have developed their own age verification systems in response to this requirement, typically using government-issued documents such as passports or driver's licences. For example, in 2019, Tinder's Japanese arm implemented a requirement for users to upload a driver's licence, passport or health ID for review to verify they were 18 and over, prior to being able to chat with matches.[735] In 2021, following the successful roll out of photo ID verification in Japan, Tinder announced all global users could voluntarily opt-in to ID verification, except where mandated by law.[736]

In addition, mobile phone company NTT Docomo allows the actual user of a mobile phone (such as a child) to be registered with the company, in addition to the account holder (often a

[729] SK Telecom, *'Press Release: Digital Driver's License Service Now Available in Korea through Identity Authentication App PASS'*, SK Telecom website, 2023, https://www.sktelecom.com/en/press/press_detail.do?idx=1466

[730] T Phillips, *'Korean MNOs let users add digital national ID card to mobile verification app'*, NFCW website, 2022, https://www.nfcw.com/2022/11/15/380341/korean-mnos-let-users-add-digital-national-id-card-to-mobile-verification-app/.

[731] F Hersey, South Korea's digital identity blockchain prepares to add new credentials, go international, 2022.

[732] Japanese Cabinet Office, 'Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People (Unofficial translation)', Japanese Cabinet Office website, 2009, https://www8.cao.go.jp/youth/youth-harm/law/pdf/for_english.pdf.

[733] Japanese Cabinet Office, Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People, Article 5 (Unofficial translation), 2009.

[734] Japanese Cabinet Office, Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People, Article 2 (Unofficial translation), 2009.

[735] Tinder, '*Tinder Commits to ID Verification for Members Globally, a First in the Dating Category*', 2021, https://au.tinderpressroom.com/idverification; Tinder, '*Age verify to chat with matches*', Tinder website, n.d., https://www.help.tinder.com/hc/en-us/articles/360041821872-Age-verify-to-chat-with-matches.

[736] Tinder, '*Tinder Will Add ID Verification Option Following the Successful Rollout of Photo Verification*', Tinder website, 2021, https://www.tinderpressroom.com/2021-08-16-Tinder-Commits-to-ID-Verification-for-Members-Globally,-a-First-in-the-Dating-Category.

parent).[737] They can do so by presenting a driver's licence, student ID card, or other document that verifies the user's name and date of birth. This allows NTT Docomo to apply age-appropriate safety settings, and to offer targeted services for younger users. It also allows for cross-account verification. For example, Line, a Thai-based social media site and one of Japan's most popular messaging and social media apps, requires users to undertake account-based verification through a user's mobile phone service provider.[738] This law also requires providers to implement measures necessary to improve the performance of and disseminate the use of content filtering software.[739]

This approach could be considered for an Australian context, where often only the account holder's details are typically known to mobile phone companies.

Age Estimation and Verification for Other Age-Restricted Products

Behavioural biometrics company Nviso Japan and age estimation provider Privately have recently announced a partnership covering digital kiosks that sell age-restricted products in Japan.[740] Privately's facial and voice analysis systems will be used to estimate the age of customers without retaining any personal information. This will enable Nviso's AI-based digital avatars to interact with customers in an age-appropriate way and prevent children from purchasing adult products and services.[741]

The Japanese government is considering the use of a chip-enabled national identity card called the 'My Number card' in the context of age-restricted sales in grocery stores and supermarkets. 'My Number cards' are linked to the holder's individual 12-digit ID number and supported by an app which enables users to obtain and store official documents on their smartphone.[742] Uptake has been slow, based on concerns relating to privacy, data security and app usability. At this stage it does not appear that 'My Number cards' have been considered for broader online age verification purposes.

[737] DOCOMO, '*Registering User Information*', DOCOMO website, n.d., https://www.docomo.ne.jp/english/support/procedure/change_release/user_registration/.

[738] LINE Safety centre, *'To connect with your family and friends safely',* LINE Safety centre website, n.d., https://linecorp.com/en/safety/family.

[739] Japanese Cabinet Office, Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People, Article 1 (Unofficial translation), 2009.

[740] NVISO, '*Press release - Revolutionizing Age Verification: NVISO Japan and Privately SA Join Forces for Cutting-Edge AI Technology in Digital Kiosks*', NVISO website, 2023, https://www.nviso.ai/en/news/revolutionizing-age-verification--nviso-japan-and-privately-sa-join-forces-for-cutting-edge-ai-technology-in-digital-kiosks; https:/www.biometricupdate.com/202302/nviso-privately-partner-to-integrate-age-verification-solution-into-emotion-sensing-japanese-retail-kiosks.

[741] A Macdonald*, 'Nviso, Privately partner to integrate age verification solution into emotion-sensing Japanese retail kiosks',* Biometric Update.com website, 2023, https://www.biometricupdate.com/202302/nviso-privately-partner-to-integrate-age-verification-solution-into-emotion-sensing-japanese-retail-kiosks.

[742] W Fee, 'T*he government wants you to get a My Number card. Should you?*', The Japan Times, 2022, https://www.japantimes.co.jp/news/2022/10/23/national/my-number-card-explainer.

The Philippines

In the Republic of the Philippines, the *Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act* (Republic Act 11930) aims to protect children from all forms of sexual violence, abuse and exploitation, especially those committed with the use of information and communications technology.[743] It includes a provision requiring all online providers of adult content to employ anonymous age verification.[744]

Following its passage in July 2022, the National Telecommunications Commission (NTC) has been granted one year to complete a policy study on age verification controls by internet intermediaries (including ISPs, web hosting, search engines and portals, internet sites, chatrooms, newsgroups, payment providers, social media intermediaries) for restricting children's access to pornographic content.

The NTC's recommendations will inform rules and regulations, to be made within 18 months after passage, governing the adoption of age verification measures in line with the *Data Privacy Act* of 2012.

Canada

In Canada, legislation has been introduced that would require organisations to use age verification methods before making sexually explicit material available online for commercial purposes. It would also make it an offence for a provider to make sexually explicit material available to a young person. Introduced in November 2021, Bill S-210 proposes that organisations who commit the offence could be liable for up to C$500,000.[745] At the time of writing, the Bill is being debated in the Canadian parliament.

International Cooperation

As noted in chapter 5, an individual's access to, experience with, and understanding of online pornography can differ significantly depending on their social, cultural and geographic context. However, internet and digital services providers operate globally and provide services to people across jurisdictions simultaneously. As such, international collaboration between governments and regulators is critical and effective policy approaches will require partnership between government and industry.

[743] Congress of the Philippines, '*Republic Act No. 11930 Section 2*', The LawPhil project website, 2022, https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html.
[744] Congress of the Philippines, Republic Act No. 11930 Section 35, 2022.
[745] Senate of Canada, '*BILL S-210: An Act to restrict young persons' online access to sexually explicit material',* Parliament of Canada website, 2021

Consultations revealed concern from some industry stakeholders that conflicting or confusing regulatory requirements from multiple jurisdictions would likely impact on compliance. Stakeholders called for the international harmonisation of regulation and standards to allow interoperability across national ecosystems and frameworks.

Cross-Sector Collaboration

In November 2022, the French Government announced the Children's Online Protection Laboratory, a sandbox which explores solutions for improving the safety of minors in the digital environment. This includes looking at appropriate age for accessing content, harassment, digital literacy, parental support, privacy protection, transparency, and moderation, with a particular focus on gender-based risks. The initiative aims to bring together technology companies, researchers and government to test possible solutions, led by a steering committee which will set priority themes each year.[746]

EU Working Group on Age Verification

Regulators in Europe, including those from the UK, France, Germany and Cyprus, meet regularly to share best practice on regulatory approaches to age verification and work towards international consensus.[747] Common challenges identified include:

- difficulties in regulating companies that operating in multiple jurisdictions, especially for smaller regulators.
- platforms changing domain names and creating mirror websites to avoid regulation, thus creating duplicative, resource-intensive legal processes.
- challenges in obtaining quantitative data on the harms associated with pornography to underpin justification for stringent age verification.
- the existence of a 'complexity trap' where the potential issues associated with age assurance hinder progress and some platforms may utilise this to delay implementing age verification solutions.
- platforms raise competition concerns as another reason to delay implementing age verification.
- difficulties in implementing age-appropriates measures based on differing developmental needs.
- public confusion and conflation regarding blanket restricted access to online pornography and measures which prevent children's access.

[746] Elysee*, 'Laboratory for Childhood Protection Online Charter',* Elysee website, 2022, https://www.elysee.fr/en/emmanuel-macron/2022/11/10/laboratory-for-childhood-protection-online-charter; see Appendix 5.
[747] Ofcom, Ofcom's first year of video-sharing platform regulation, p19, 2022.

Some of these challenges can be mitigated through media literacy efforts and public awareness campaigns.

Global Online Safety Regulators Network

In 2022, eSafety worked alongside Ofcom, the Broadcasting Authority of Ireland and Fiji's Online Safety Commissioner to establish the Global Online Safety Regulators Network (the 'Network'). While the Network does not have a specific focus on the harms caused by online pornography, it is the first international network dedicated to online safety regulation. The Network will encourage wider international membership and cooperation, with the aim of ensuring approaches to online safety between countries are as consistent and coherent as possible.[748]

Conclusion

This chapter provides an overview of international legislative, regulatory, and technical developments relating to children's access to online pornography. While not an exhaustive summary of undertakings across all countries, it highlights that many countries have acknowledged that children have the right to experience digital environments in an age-appropriate manner. The policies and legislation outlined in this chapter are focused on identifying child users to minimise harm and protect their safety and privacy.

Although technological solutions for restricting children's access to online pornography (and other age-restricted goods and services) differ across countries, there are common, overarching principles that aid policy direction, namely: proportionality, accuracy, transparency, security, compliance with laws, data minimisation and privacy protection.

Countries which have passed relevant laws face enforcement challenges (including financial penalties for non-compliance), highlighting the importance of international collaboration and coordination. Collaboration between internet, telecommunications and privacy regulators also surfaces as an essential component to ensuring principles are effectively enforced. Policies

In several countries, age assurance and verification technologies are being supplemented with other measures, demonstrating that there is no single technological solution to prevent children from accessing online pornography. Involving mobile phone companies and device manufacturers in limiting access to age-restricted goods and services or enabling parental controls on devices provides a complementary means to safeguarding children in digital environments.

[748] eSafety Commissioner, '*The Global Online Safety Regulators Network*', eSafety website, n.d., https://www.esafety.gov.au/about-us/who-we-are/international-engagement/global-online-safety-regulators-network.

Chapter 11: Other technological interventions (complementary measures)

Key points

- Age assurance is one key component of any effort to keep children safe from a range of online harms, including those associated with access to pornography. Ascertaining a user's age is most beneficial when provides a foundation for further measures that create safe and age-appropriate experiences.
- Age assurance needs to be coupled with other complementary measures – both educational and technological – to mitigate potential online harms to children. Different measures will be suitable depending on a child's age and developmental stage, as well as the context in which they experience content.
- Complementary measures are likely to offer the strongest protection when cross sections of the online industry are working together.
- This chapter explores a range of relevant complementary measures available and commonly in use by industry, including:
    - Filters, parental controls and other privacy and safety settings. These tools are available broadly – on devices, as built in features to services or through third party software. Issues around cost, accessibility, and how accurate these tools are may be impacting parental and user uptake.
    - Content moderation, which can be done either by algorithms or human moderation. Both approaches have their benefits and limitations – including proportionality, managing biases and dealing with content at scale.
    - Other approaches, including providing safety and educational material, tools such as nudges and reporting capabilities as well as tools which allow users control over their online experience can also be used by industry in a layered approach to preventing children's access to harmful or age-inappropriate material.

Overview

In addition to exploring age verification, the Committee asked eSafety to consider 'complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms' associated with children encountering online pornography. The previous government's response highlighted 'filtering and other proactive user safety settings' as two types of complementary measures that can play an important role in achieving this goal.[749]

This chapter explores complementary measures to prevent and minimise harm to children. To provide a holistic approach, eSafety considered the different contexts in which children encounter online pornography. Our research shows this happens both intentionally and unintentionally and across pornography sites, social media feeds, and through messages and group chats.

While user safety is a shared responsibility, the burden of safety should never fall solely upon the user. Services should develop effective proactive measures and moderation systems to support user safety by preventing harms before they occur. Services should assess the level of risk that children could access pornography on their service and put in place proportionate measures to address that risk.

For pornography sites, conducting age assurance and restricting access to those who can establish they are 18 or older is an important – though not foolproof – way to reduce children's access to online pornography. There are a range of other complementary measures which can also help reduce this access by preventing children from ever arriving at pornography sites. These measures are strongest when different sections of the online industry are working together towards this shared goal. For example, filters are enabled on devices, networks or browsers, pornography sites are tagged as such so they are picked up by these filters, safe search settings are turned on so pornography is not surfaced in searches, and the messaging services through which links to pornography can be shared with children have settings enabled to block this content.

For social media and many other online services, the minimum access age is often 13 years. Many, though not all, of these services prohibit adult content such as online pornography. For these services, a range of measures can aid the enforcement of relevant policies and prevent children from encountering content that is not age-appropriate, including:

- proactive moderation, such as tagging or removing content and activity

[749] Australian Government, '*Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence',* Parliament of Australia, 2021, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Government_Response.

- preventing underage users from accessing or being served with such content
- providing reporting mechanisms to flag violations.

Other complementary measures include a combination of child supervision, safety discussions, and using filters, safety settings, and parental controls. There are a range of factors to consider, including the ability to calibrate different experiences and permissions for children which can be adjusted as their capacities evolve, whether safety measures are in-built and on by default, and how to reduce any barriers to third-party safety measures. Our research and consultations demonstrate that adults need greater support to access, understand, and apply these measures. Barriers including cost, low awareness, and digital literacy also continue to hamper efficacy and need to be addressed – both the online industry and government can assist parents and carers in overcoming these barriers.

As children grow up, it becomes more likely they will be able to bypass filters and parental controls if they want to do so. Accordingly, education about online pornography, consent, and respectful relationships remains a crucial complementary measure for preventing and minimising harm. This is explored in chapter 13.

While older children may be more likely to seek out online pornography, our research shows they are also experiencing 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.

Filters, safety and privacy settings, and parental controls

There is a clear role for parents and carers supervising their children's use of the internet and engagement in online environments. Supervision can be achieved through a variety of means, though is often supported by parental controls and filters. **Filtering** can be used to block access to content that may be illegal, harmful, or not age appropriate.[750] **Parental controls** are predominantly software tools that allow you to monitor and limit what your child sees and does online.[751] They can also be built into products which allow parents to control child accounts (for example – Google's Family Link).

Third party parental controls can be installed on home Wi-Fi systems or on individual devices. They can also be set up to do things like:

- Block children from accessing specific websites, apps or functions, such as online pornography websites.
- Filter content — such as 'adult' or sexual content, and illegal or age-restricted content that may promote self-harm, eating disorders, violence, drugs, gambling, racism and terrorism.
- Allow parents and carers to monitor a child's use of connected devices, with reports on the sites they visit and the apps they use, how often and for how long.
- Set time limits for being online.
- It is also possible to enable browsing in 'safe mode' and with 'safe search' filters. Many platforms, devices, and streaming services feature options for parental controls or filtering.

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. They can be adjusted by parents using parental controls or applied by a user of any age to their own account.

Such tools are not only useful for parents of children. They can be used by adult users looking to exclude content that they do not wish to engage with (this could include online pornography or gambling).

[750] Tech Target, What is content filtering and how does it work?, n.d., https://www.techtarget.com/searchsecurity/definition/content-filtering.
[751] eSafety Commissioner, '*Parental Controls', n.d.,* https://www.esafety.gov.au/parents/issues-and-advice/parental-controls.

Many of the stakeholders we consulted with supported the use of device-based safety measures, such as parental controls and filters. They noted these tools can be highly effective at filtering out pornography, especially when adult sites apply labels to facilitate filtering.

Where and how is it currently applied

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 may be available for free or at a cost. These technologies can be applied at various levels, including device- or operating system-level, browser-level, account-level, or network-level.

Some content filter products or services can be configured by selecting a child's age range or age gate limit. The filter provider then sets and applies the criteria it considers appropriate for each age range, providing a proportional approach to content filtering. Some content filters allow finer adjustments of filtered content across categories such as adult content (including pornography, gambling, alcohol). While this level of granular control may be beneficial for more digitally literate parents or carers, those without the necessary skills, or those wanting a quick fix to controlling their children's internet access may overlook these controls.

If a device or program is shared by multiple members of a family, controls may be available to adjust privacy and safety settings to reflect each user's age and skills. Although online platforms and services have faced difficulties in keeping pace with moderating and classifying of new content available, many have sought to provider safer 'kid friendly' environments and content for younger audiences. Online streaming services who allow user generated content, such as YouTube Kids offers family friendly content along with parental controls that can set time limits on apps and turn off search functionality. Major device manufacturers Apple and Google include parental control options in their operating systems for child accounts.

Apple Parental Controls for iPhone, iPad, and iPod Touch

Apple users can invite family members to share services such as Music through Family Sharing. The organising adult user can create accounts for children.

Used in combination with Screen Time, parents who set up their children's account sunder Family Sharing can review their child's activity reports and set time limits for specific apps from their own devices. Parents can also:

- set age-related restrictions for content in apps, books, TV shows and films
- prevent their child from being able to install or delete apps or make in-app purchases
- filter website content to limit access to adult content in Safari and other apps, including by adding specific websites to an approved or blocked list, or limiting access to only approved websites.

Parents can seek to prevent their child from making any changes to these settings by protecting them with a passcode linked to their own Apple ID and password. This is not contingent on a child being under the age of 13.

Again, when a child turns 13, they are permitted to maintain their own Apple ID account without participating in Family Sharing, regardless of their parents' views.[752]

Communication Safety

In June 2023, Apple announced its expansion of its Communication Safety tool, which scans messages locally on children's accounts/devices to flag visual content that contains nudity. The feature is expanding to more communication methods, including AirDrop. Apple does not see the images scanned.

The tools will soon be turned on **by default** for all child accounts on a Family Sharing plan, but can be disabled by parents. Discord has said they intended to incorporate the API into their iOS app, enabling the use of the tool on its platform.[753]

[752] Apple, '*Family Privacy Disclosure for Children*', n.d., https://www.apple.com/legal/privacy/en-ww/parent-disclosure/#:~:text=Once%20your%20child%20reaches%20the,without%20participating%20in%20Family%20Sharing.

[753] L H Newman, '*Apple Expands Its On-Device Nudity Detection to Combat CSAM*', Wired, 2023, https://www.wired.com/story/apple-communication-safety-nude-detection/.

Google Family Link

Google's Family Link App can be run on certain Android devices and iPhones held by parents and used to supervise certain Android devices held by children. It allows parents to create and supervise a Google Account for a child under 13 or add supervision to a child's existing account. This will automatically activate SafeSearch on the child's account to filter explicit content from search results.

Family Link allows parents to:

- approve or block specific apps for download in Google Play
- choose a supervised experience on YouTube, or YouTube Kids
- apply data sharing and privacy settings, including whether apps can access the device's microphone, camera or contacts

When a child turns 13 (or the applicable age in their country, as set by local law),[754] they have the option to turn off parental supervision or to allow their parent to continue managing their account. Google does not allow parents to override this decision.

Filtering software that is installed directly on a device and is integrated into browsers, is commonly used. In Australia, a list of third-party accredited filters can be found under the *Family Friendly Filter Scheme*. The scheme assesses internet content filtering product effectiveness and whether the vendor updates their filter in line with eSafety's Prohibited URL Filter (PUF) list.[755]

Content filtering at the internet service provider level has traditionally not been a popular choice with the Australian public or internet providers. Internet providers claim that implementing and delivering granular parental filtering controls to their customers is cost prohibitive and may affect the performance of service to all customers.[756] This claim was last independently tested in Australia in 2009 and although performance impact was found to be minimal, the technologies implemented by service providers were also found to be easy to circumvent.[757]

eSafety is not aware of any Australian ISPs which apply filters or parental controls by default. Some Australian internet service providers may provide upstream filtering using Interpol's

[754] In Australia, the age is currently 13.
[755] Communications Alliance, 'Family Friendly Filters', n.d., https://www.commsalliance.com.au/Activities/ispi/fff.
[756] Internet Society, '*Internet Way of Networking Use Case: Content Filtering*', 17 December 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-content-filtering/.
[757] Trevor Clarke, '*ISP-level filter trial vendor happy with results*', Computerworld, 2009, http://www2.computerworld.com.au/article/330034/isp-level_filter_trial_vendor_happy_results/?utm_medium=rss&utm_source=tagfeed.

'Worst Of' list for their subscribers. The 'Worst Of' list contains domains that distribute child sexual abuse material and which have been verified by at least two national agencies.[758]

Family Friendly Filters

The Family Friendly Filters program is operated by the Communications Alliance, an association which represents the Australian communications industry, including ISPs.[759] 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.

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 map 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[760]
- Class 1: Recommended for children over 15 years of age[761]
- Class 2: Recommended for children between 10 and 15 years of age[762]
- Class 3: Recommended for children under 10 years of age[763]

RTA Tagging

The American organisation Association of Sites Advocating Child Protection (ASACP) created a 'Restricted to Adults' voluntary label.[764] The label is applied as a HTML meta tag within the header of websites. This label enables the site to be filtered by a range of tools, including browsers, ISPs, firewalls, plugins, operating systems and commercial

[758] Interpol, Blocking and categorizing content, https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

[759] Communications Alliance, 'Family Friendly Filters'.

[760] These filters block websites on the eSafety Prohibited URL Filter (PUF) list, which contains approximately 21,000 URLs where eSafety has located child sexual abuse material following complaints from the public. Any filter which does not block at least 97% of the URLs on the PUF list automatically fails and does not receive classification.

[761] In addition to blocking at least 97% of sites on the PUFs list, these filters must block at least 55% of sites on the TestLab's harmful categories list, and not more than 5% of the control list.

[762] In addition to blocking at least 97% of sites on the PUFs list, these filters must block at least 70% of sites on the TestLab's harmful categories list, and not more than 10% of the control list.

[763] In addition to blocking at least 97% of sites on the PUFs list, these filters must block at least 80% of sites on the TestLab's harmful categories list, and not more than 20% of the control list.

[764] ASACP, Restricted to Adults label.

filtering software. The ASACP website includes a list of filtering products and services which recognise the tag.

Many of the stakeholders eSafety spoke with in the adult industry said they have used this labelling on their site.

Some home routers have parental control settings that provide control over the time children can access the internet as well as websites that can be accessed (such as a set number of hours per day or daily permitted and blocked times). These settings offer similar configuration options to internet content filters but require a parent to navigate the router's login and menu system. While a smart router may provide adequate control at home, older or more digitally literate children can still view blocked content once they connect their device to a mobile network or unfiltered internet service.

Some major mobile phone networks in the UK filter adult content by default, following guidelines developed by the British Board of Film Classification (BBFC) for customers when going online via a mobile connection.[765] To disable these filters, customers must verify their age by either visiting a store in-person with identity documents or providing credit card details on a mobile app or over the phone. According to Ofcom's research, just over a third (35%) of parents with children aged 3-17 said the adult content blocker was in place on their child's mobile phone.[766]

Safety and Privacy settings

Good practice for default safety and privacy settings for children include having safe mode filters on, placing user data on the highest privacy setting and limiting access to the user's device.

Providing users with knowledge of default settings on a platform or service and how to change those settings is an important user empowerment measure and support users to have safer online experiences.

When users attempt to change or update their default settings, explanations and prompts should be provided in plain language so that the implications of changes are fully understood.

Placing the highest privacy settings on user accounts by default, can prevent bots or bad actors from sending pornographic content to users. In eSafety's research, 28% of participants who had

[765] British Board of Film Classification, '*Mobile phones and filters*', available at: https://www.bbfc.co.uk/about-classification/mobile-content.

[766] Ofcom, '*Children and parents: media use and attitudes report 2022*', p.65, 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf.

seen online pornography had been sent it by someone without their permission.[767] Some focus group participants reported receiving messages on social media from spam or fake accounts that would send them pornography.

Sensitive Content Warnings

Apple has announced plans to expand its Communications Safety tools for adults. Adults can turn on a setting which would blur incoming messages or content if they contain nudity and ask users if they want to see the content. All processing occurs on device so Apple does not get access to the content.

Effectiveness

Lack of uptake from parents and child circumvention of content filters can limit the effectiveness of these tools.

Parental uptake

According to recent research commissioned by the Department of Infrastructure, Transport, Regional Development and Communications, 45% of parents and carers in Australia do not use any parental controls.[768] 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'.[769]

Most parental controls and filters need to be installed and configured by parents. This presents challenges, as children that are vulnerable online are generally more vulnerable offline.[770] Vulnerable children are less likely to have parents or educators who have the capacity to engage with them in relation to their internet use. There is also a clear generational gap in **digital literacy**.[771]

In France, devices with operating systems such as computers, tablets and smart watches will soon be required to be sold with parental control systems pre-installed and ready for use. They systems are not required to be activated by default, but consumers who are parents of children

[767] eSafety, forthcoming.
[768] Department of Infrastructure, Transport, Regional Development and Communications, '*Report on classification usage and attitudes research*', p.43, 2022, https://www.classification.gov.au/sites/default/files/documents/5270_ditrdc_classification_usage_publication_report_finalv2.pdf.
[769] Department of Infrastructure, Transport, Regional Development and Communications, '*Report on classification usage and attitudes research*', 2022.
[770] S Livingstone, '*Vulnerable offline and at risk online: tackling children's safety*', LSE Blog, 20 February 2019, https://blogs.lse.ac.uk/parenting4digitalfuture/2019/02/20/vulnerable-offline-and-at-risk-online/.
[771] UNESCO, '*Digital Age Assurance, Age Verification Tools and Children's Rights Online across the Globe: A Discussion Paper',* 2021, p.50.

should be made aware of the features and supported to turn them on at the point of sale. To this end, Law 2022-300 requires device manufacturers to sell devices that enable the activation, use and de-installation of parental controls at no extra cost. Controls are to be easy to access and understand and protective of children's data.[14]

To minimise harm, safeguards should be built into online products and services accessible to children, by default. Additional education about parental controls in a variety of formats and languages is also necessary.

Circumvention

Technically savvy children may be able to turn off or bypass filtering services to access content they should be prevented from viewing. Children can also use a VPN to bypass content filters as use of a VPN removes geo-blocking and parental control filters which are tied to an IP address.

Device-level parental controls offered by Apple and Google both allow children to turn off parental controls at age 13.

The risk of over-blocking

One of the shortcomings in using content filters is the risk of over-blocking, that is, preventing access to sites that the child should be able to view. For older children and teenagers, this may include content related to sexual health and support services, including resources for members of the LGBTIQ+ community. While some content filters do allow children to request to view block websites, this reactive approach risks infringing on privacy.[772]

Accuracy testing

Enex TestLab tested a minimum of 1500 URLs against internet content filtering solutions available on the market.

The accuracy rate of each internet content filter is determined by comparing the rate of blocked URLs on the Enex TestLab RX list (websites refused classification under the Classifications Scheme) and the blocked URLs on the control list (regular websites that should not be blocked). Where a greater percentage of RX material is blocked, a proportionally larger amount of blocking of control material is allowed.

[772] United Nations, *'Convention on the Rights of the Child*', 1989, https://www.unicef.org/child-rights-convention/convention-text.

Options tested: Software-based filters

McAfee Safe Family

The McAfee Safe Family app is available on Windows, Android and iOS. Features vary depending on the platform. The filter is managed by installing the app on a parent's device (when installing the app on each device, the user indicates whether it is a parent's or child's device.) The installation process is guided with the installation wizard, upon completions set up the child's age profile and select any extra categories to block or allow. As well as filtering web content, the app can track the location of a device (and thus the child) and when and what usage is occurring on the device.

The McAfee Safe Family app is included in Optus' Family Plans and Kids Plans.[773] Customers can opt-in to the subscription at the timing of signing up or anytime after in the MyOptus app.

Norton Family

Norton Family is a software filter. To set it up, a parent registers online and then downloads the software from a link provided. The straightforward parental control setup process involves establishing the child's profile, blocked categories and time restrictions. Enex TestLab evaluated Norton Family with the default installation and blocked categories. Norton Family is available for Windows PCs and iOS and Android mobile devices. Enex TestLab did not test any mobile devices. They did not evaluate the browser extension because it might not be installed by all users and could be easy for a child to circumvent by installing another browser.

Options tested: Device based filters

ASUS ZenWiFi Pro XT12

The ASUS ZenWiFi Pro is a router with content filtering functionality provided by Trend Micro. The router requires an iOS or Android device to set up. Once the hardware is configured, parental controls can be set up and adjusted by mobile device or a PC on the network. Under parental controls, the web filter provides four category choices, each with at least two subcategories:

- adult and mature content (presumably over 18) and sites that contain material of a sexual, violent or illegal nature
- instant messaging and communication
- peer-to-peer and file transfer services
- streaming and entertainment sites.

[773] Optus, '*Family Hub*', available at https://www.optus.com.au/support/family-hub.

The router can also manage a user-specified deny or allow list but not both, with a maximum of 64 sites. This item is configured under the firewall settings as URL Filter. Time scheduling can be configured under parental controls, with start and end times for weekdays and weekends or individual days in 15-minute increments.

McAfee Secure Home Platform

McAfee Secure Home Platform is a router-based filter. It requires an iOS or Android device to complete setup. The setup process involves setting the child's age and blocked categories and assigning these to the child's devices.

To increase protection, parents can also install a secondary application named McAfee Web Advisor on Windows devices. McAfee Web Advisor is a browser extension that works with the Secure Home Platform router to ensure sites are blocked. Enex TestLab tested with a Secure Home Platform router and Web Advisor installed.

Results

As the table below demonstrates, the software-based solutions (Safe Family and Norton Family) were generally more accurate than the device-based solutions. Importantly, the ZenWiFi Pro XT1 router did not met the necessary thresholds to pass the Family Friendly Filter.

	Safe Family	Norton Family	ZenWiFi Pro XT1	Secure Home Platform
% blocked – control list	7.7%	6.4%	3.6%	6.8%
% blocked – RX list	81.8%	81.1%	58.2%	76.9%
% blocked eSafety PUF list	99.2%	97.1%	94.2%	97.8%

Perspectives on system-level filters and parental controls

Consultation stakeholders supported greater promotion of parental controls and filtering but stated that reliance on these measures alone would not be sufficient. They emphasised that these measures have existed for years, but to date, have not been effective in preventing children's access to online pornography. Some stakeholders were also of the view that parental controls and filters may provide a more targeted response than blocking sites at an ISP-level as this could censor whole domains. If ISP-level measures were to be considered, stakeholders felt they should be opt-in measures for consumers rather than automatically applied.

Issues of over-blocking and circumvention may be exacerbated by the perceived or actual lack of flexibility within available device-level tools to allow for dynamic adjustments as children grow older and more mature. Some stakeholders felt that filters and parental controls take a rigid, heavy-handed approach that leans toward prohibiting questionable material for anyone under the age of 18. They argued that the difference between a 12 year old and a 14 year old can be substantive, and that 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.

Use of parental controls should be informed by the evolving capacities of a child (such as age, digital literacy skills and maturity). As children get older, a graduated approach to use and easing controls is often needed. For example:

- Very young children under 5 years old have very basic online safety awareness, critical digital literacy skills and capabilities – therefore stronger parental device-based filters are required as safeguards for the child.
- As children reach approximately 12 years old and reach secondary school, open discussions and greater online safety education is needed regarding age-restricted content and online behaviours.
- For teenagers, strong default settings and filters may be overly restrictive. In such circumstances, a gradual reduction in the use parental controls and increased use of user empowerment tools (such as mute, block and self-filtering content) can support user safety, by allowing the user to navigate online environments in a safe setting, rather than seeking to circumvent parental controls together.[774]
- Enhanced educational opportunities for users that provide a better understanding of safeguards available (particularly for parents and carers) must continue to evolve alongside technologies and online environments.

[774] Based off eSafety guidance on parental controls – further resources might be required. eSafety Commissioner, *'Online Porn',* n.d., https://www.esafety.gov.au/parents/issues-and-advice/online-porn

Content moderation

Content moderation refers to the systematic practice of vetting content posted online to determine its appropriateness.[775] Content moderation is fundamental for removing content that violates terms of service, content policies and community guidelines.

For services that do not allow pornography, content moderation can help to detect, reduce and remove pornographic content even at point of upload, minimising the risks to children. For services that allow adult content, content moderation combined with age assurance can create more age-appropriate experiences if users under 18 are permitted on the service.

Broadly defined, content moderation involves detection through a variety of processes, including:

- algorithmic detection through machine learning technologies that identify and block inappropriate content
- human content moderators who review and classify problematic material
- community moderators who report content or take enforcement action
- users reporting of inappropriate content or underage users.

As identified by Enex TestLab, prominent issues regarding content moderation involve the difficulties that larger social media companies experience when actively monitoring and policing content for a global user base. Sometimes harmful content is only taken down after complaints or negative publicity surface. See **Appendix 8** for more information.

While the criteria for content that is moderated varies across services depending on their terms and guidelines, categories such as sensitive content (for example nudity and sexually explicit material) and illegal content are often used.[776]

Where and how is it currently applied

Algorithmic content moderation

Algorithmic content moderation involves automated or artificial intelligence-based system used to classify, detect, and respond to illegal and harmful material.[777] With increasing scales of content and greater user and regulatory pressure to reduce harmful content, digital services increasingly rely on algorithmic content moderation.

[775] All tech is Human, '*AI and Human Rights*', 2022, https://alltechishuman.org/ai-human-rights-report.
[776] All tech is Human, AI and Human Rights, 2022.
[777] E Pirkova, M Kettemann et al, '*Spotlight on Artificial Intelligence and Freedom of Expression A Policy Manual*', Office of the Representative on Freedom of the Media Organization for Security and Co-operation in Europe, 2021, https://www.osce.org/representative-on-freedom-of-media/510332.

Research commissioned by the Australian digital industry identified that 53% of respondents believed online services should scan for and remove pornography.[778]

> 'Better moderation is always beneficial, and this will probably come with time as algorithms improve over time' – eSafety focus group participant, 16

Digital services often rely on three broad categories of algorithmic content moderation:[779]

Matching models: which detect matches between new posts and known material recorded on a database as compact and manageable digital fingerprints.

Predictive models: which uses machine learning to classify new posts against platform rules. They find patterns and characteristics of new or previously unknown content based on training data. Predictive models are best suited for situations where training data is both ample, comprehensive, and is often used for identifying more objective features like nudity.[780]

Algorithms can also target **metadata and behavioural signals** to detect certain content and accounts for review. This includes data on account and user information, access frequency and device information.

Examples

According to **Facebook's** transparency reports, between October and December 2022, Facebook acted on 29.2 million pieces of adult nudity and sexual activity content. Of this, 94.1% was actioned before people reported it.[781]

Xbox reported that between January and June 2022, it proactively acted on 199 thousand instances of adult sexual content. Of the total instances of enforcement on adult sexual content, 24% occurred proactively.[782]

[778] DIGI research 53% of respondents said that online services should scan for and remove pornography, https://onlinesafety.org.au/wp-content/uploads/2022/10/R220719-DIGI-CA-Project-Class-1-Sep-2022-Survey-Results-PUBLIC-RELEASE.pdf

[779] E Douek, '*Governing Online Speech: From 'posts-as-Trumps' to Proportionality and Probability*', Columbia Law Review 121, no. 3, 2021, https://columbialawreview.org/content/governing-online-speech-from-posts-as-trumps-to-proportionality-and-probability/; C Shenkman, D Thakur, E Llansó, *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis*, Center for Democracy & Technology, 2021, https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/.

[780] Shenkman, et al., Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis, 2021.

[781] Meta, '*Transparency Center, Adult Nudity and Sexual Activity*', accessed 8 March 2023, https://transparency.fb.com/en-gb/policies/community-standards/adult-nudity-sexual-activity/.

[782] Xbox, '*H1 Transparency Report*', 2022, https://www.xbox.com/en-AU/legal/xbox-transparency-report.

While these tools can be effective for static content like images and text, moderating live streamed content remains challenging. For example, moderating livestreams requires intensive computation.[783] Content moderation algorithms can also be used to shape user experiences in other ways, such as demoting **'borderline content'**.[784]

Services which allow adult content can apply filters so that children – or adult users who have opted not to see this type of content – avoid certain content being recommended to them or appearing in their feed. There is limited public information within platform transparency reports on the uptake and efficacy of these tools.[785] TikTok announced that it is introducing 'thematic maturity' categorisations of its content, so that users aged 13 to 17 are not shown content with mature or complex themes.[786] Interventions such as these cannot be effective unless user accounts are marked with the correct ages or age ranges, which requires robust age assurance.

Safe Search

Safe search is a search engine filter that blocks explicit content such as pornography. Major search engines – including Bing, Duck Duck Go and Google – offer safe search options. A child can circumvent safe search by disabling it or using another search engine. Google's parental controls allow parents to enable safe search capabilities for their children's accounts.

Community-based content moderation

Community moderation is the process of users moderating content within a community, and is common in many large platforms, such as Twitch, Reddit, Discord and Facebook. Community moderators enforce the rules and norms of specific communities using tools the platform makes available to them (such as removing users from communities or deleting posts). On platforms such as Reddit, individual communities (subreddits) may have substantially different rules, norms and values to each other, on top of Reddit's own rules. Community moderators apply their own contextual understanding of the community to enforce these rules.[787]

Community moderation isn't just about managing bad behaviour. It also provides opportunities to encourage, incentivise and foster good behaviour. A well-moderated community can create a safe space where members feel welcome, supported, and respected. Despite its benefits, given

[783] Shenkman, et al. Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis, 2021.
[784] Shenkman, et al. Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis, 2021.
[785] For example, Twitter's ('X's) transparency reports do not report on aspects of moderation practices, such as demoting content.
[786] C Keenan, '*More ways for our community to enjoy what they love*', TikTok Newsroom, 13 Jul 2022, https://newsroom.tiktok.com/en-us/more-ways-for-our-community-to-enjoy-what-they-love.
[787] A LL Cullen, S R Kairam, '*Practicing Moderation: Community Moderation as Reflective Practice*', 2022, https://dl.acm.org/doi/pdf/10.1145/3512958.

the sheer scale of content posted, an over-reliance on community moderation can lead to moderation gaps, particularly in the absence of automated content moderation tools.[788]

User tagging: how tools can work together

Content can be tagged by individual users when uploading or sharing content (for example, Reddit's Not Safe For Work (NSFW) tag or Twitter's sensitive media label – which suggest the nature of the content to other users. Tagging allows the user or a moderator to judge its appropriateness, rather than leaving this to an algorithm. Services can apply additional settings, such as automatically blurring, blocking or removing content from recommendations targeting child accounts, or adult users who have opted out. These measures rely on voluntary efforts and their effectiveness may vary depending on the platform or community and whether services enforce and encourage their use.

These measures can be complemented by tools which detect sensitive, untagged content and can alert moderators. Appropriate age-assurance measures for identifying child users can also prevent children from searching for tagged content.

Effectiveness

Effectiveness of algorithms and human review

While algorithms help digital services to expeditiously classify, filter, flag and curate online information, they also have limitations.[789] Moderation, and particularly automated moderation, may result in under-blocking or over-blocking unsuitable content.

Where content moderation algorithms flag content or an account, it is often triaged for human review.[790] Given the limitations of content moderation algorithms, it is standard practice for human review to be incorporated into systems using content moderation algorithms.

Any form of moderation relies on the moderator's judgement and the platform's policies to determine what is acceptable. Further, any independent review and the accountability of moderation practices depend on the service provider's commitment to transparency and accountability.

[788] Arianne Gift, '*Twitter's BlueSky begins developer testing stage, highlights content moderation'*, Micky, https://micky.com.au/twitters-bluesky-begins-developer-testing-stage-highlights-content-moderation.
[789] All tech is Human, *AI and Human Rights*, 2022.
[790] R Gorwa, R Binns, C Katzenbach, '*Algorithmic content moderation: Technical and political challenges in the automation of platform governance'*, Big Data & Society, 7(1), 2020.

Requiring global digital services to rapidly detect and remove inappropriate material involves a trade-off of efficiency and timeliness for accuracy, sensitivity to context, and equities such as due process for individual users. These adjustments entail complex policy decisions that vary from issue to issue, for example, the appetite for **false positives** in detecting nudity might differ across cultures and jurisdictions. [791]

Accuracy errors occur due to a variety of reasons, including system bias, poor judgement of context and language, and limited robustness to deal with circumvention efforts or unexpected real world inputs.[792] Intensive moderation can curtail harmful content, however content moderation algorithms can also remove excessive amounts of content, particularly content that represents marginalised communities.[793] This highlights a need for accessible appeals processes to be used by platforms. Twitter previously announced an updated appeal process for 'sensitive media' violations, where a user's tweet is automatically tagged as sensitive.[794]

Third party assessment

eSafety procured Enex TestLab to conduct an independent assessment of a range of age assurance and other, complementary safety technologies available on the market. As part of this work, Enex TestLab assessed Spectrum Labs, an artificial intelligence (AI) content moderation service.

What are Spectrum Labs' services?

Spectrum Labs can be configured with a range of AI modules which detect and moderate various types of content and activity in real time as it is posted to a service. This includes detecting underage users (for example, those who post information which indicates that they may have created their account with a false age) as well as detecting sexual content. Depending on the client's configurations, such accounts or content may be automatically actioned (for example, suspended or removed) or sent to the client's human moderators for vetting and action under the terms of service.

Assessment methodology

Enex TestLab noted that a content moderation technology needs to be installed in a client's online ecosystem and trained to work with the characteristics of the service it is being used to monitor. Conducting statistically meaningful testing would require the

[791] E Douek, '*Content Moderation as Administration*', Harvard Law Review Vol. 136, 10 January 2022.
[792] Shenkman, et al. Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis, 2021.
[793] T Lorenz, '*Internet 'algospeak' is changing our language in real time, from 'nip nops' to 'le dollar bean''*, The Washington Post, 8 April 2022, https://www.washingtonpost.com/technology/2022/04/08/algospeak-tiktok-le-dollar-bean/.
[794] Twitter Support, '*Tweet on 4 Aug 2021*', twitter.com/TwitterSupport/status/1422652336430854144.

cooperation of an active online service with a large user base. Given this type of testing was beyond the scope and timeframes of this report, Enex TestLab assessed Spectrum Labs based on interviews with three of its clients who use it to support their content moderation efforts: a dating app, a gaming platform, and a social chat service.

Accuracy

At least two of the three clients use Spectrum Labs' underage module. One client relayed that before purchasing the module, it provided Spectrum Labs with a random log of chat streams to run a 'health check'. The client was impressed when Spectrum Labs' analysis returned a list of potential underage users as well as some examples of bullying. Following roll out of the underage module, the client now identifies an average of 5-10 users per week who are likely to be children who have used an adult's ID to access areas of the client's service intended to be restricted to adults. Across all the modules this client uses, they have found accuracy the to be between 80 and 100%, with accuracy measured by human moderators assessing content flagged by the AI. Notably, the client does not measure false negatives, or content that may have escaped detection.

Another client which uses the underage module stated that the technology was initially flagging up to 50% false positives. The client's moderators found this was related to users associating themselves with numbers which had nothing to do with their age but which the technology assumed could be age-related. Following fine-tuning to account for the service's specific context, the false positive rate has been reduced to about 25%.

The technology's error rate can be calibrated based on a client's preference. For example, one client noted a preference to err on the side of caution within the child sexual abuse material module, which may result in more false positives being flagged for review by human moderators but reduces the chances of real cases going undetected.

Privacy, security and sensitivity of data

Spectrum Labs does not require the provision of personally identifiable information, though it does rely on the ability to scan content that users post against the parameters of its modules. Spectrum Labs states that it is compliant with GDPR, CCPA, and is SOC 2 certified.[795]

[795] State of California, '*California Consumer Privacy Act (CCPA)*', https://oag.ca.gov/privacy/ccpa; European Union, *General Data Protection Regulation* (GDPR), 2016, https://gdpr-info.eu/; American Institute of CPAs, '*Soc 2*', https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.

Bias

Enex TestLab noted that the system could develop or reflect biases, but also pointed to the ability for Spectrum Labs to work with its clients understand the context of their services and userbase, and to tweak the AI over time to improve accuracy and reduce bias.

Cost

Enex TestLab assessed the cost as ‘substantial’, noting one client mentioned it would not have been able to use the product in its start-up phase.

Transparency

While Spectrums Labs does not communicate directly with users whose content is flagged, many of its clients build transparency and appeals steps into their content moderation systems to communicate with users when their content is actioned.

Overall

Enex TestLabs concluded that Spectrum Labs is successfully deployed in the marketplace with good results.

Effectiveness of community moderation

The impact and effectiveness of community moderation is variable depending on the platform or service offering and nuances in communities.

Community moderated services

Discord is a centralised messaging platform where users can communicate in private servers. While a server’s administrators or moderators are encouraged to form their own safety guidelines, all servers must adhere to Discord’s community guidelines.[796] Discord requires users to be 13 years of age and over, and a higher minimum age for specific countries. Certain servers, or channels within those servers, can be designated by their owner as age-restricted and users will need to confirm their age to view the

[796] Discord, ‘*Role of Administrators and Moderators on Discord*’, accessed 16 Feb 2023, https://discord.com/safety/360044103531-role-of-administrators-and-moderators-on-discord#:~:text=They%20can%20do%20things%20like,an%20issue%20in%20a%20server.

content.[797] Age restricted servers and channels are exempt from the explicit content filter.

Reddit operates a centralised service but relies heavily on volunteer community moderators interacting with subreddit members to manage communities. Like Discord, Reddit's individual communities or 'subreddits' can create and enforce rules as long as they do not conflict with Reddit's Content Policy.[798] Reddit also has a minimum age of 13.[799] Content that is NSFW (not safe for work) needs to be tagged as such and is blocked by default, requiring users to confirm they are 18 to view it.[800]

It can also be difficult to monitor and enforce standards of moderation consistently across a service. Many services do not provide training for volunteer moderators, and there may be limited options for assessing their compliance with any standards or guidelines. A combination of community, and other forms of proactive moderation, help capture more harmful content faster. For example, Reddit uses automated tools from Hive Moderation[801] and its administrators can intervene where community moderators fail to remove content or ban accounts for illegal or prohibited content.[802]

Perspectives on content moderation on platforms

For platforms which have a wide range of user ages, or allow some forms of adult content, effective and targeted content moderation is critical to providing safer user experiences. Age-based content moderation is most successful when age assurance tools are used to gauge a user's age. Similarly, age assurance is most effective when content moderation practices and tools consider the age-appropriateness of materials such as pornographic content.

Content moderation is not limited to scanning and deleting content. Industry should consider different and layered outcome pathways, consistent with the context of their specific platforms and communities. Content moderation algorithms and policies should be reviewed often, to make sure they are not negatively impact marginalised groups and reinforcing digital exclusion. The tools should also be paired with empathetic and timely review mechanisms and transparency in policy application and decision making.

[797] Discord, '*Age-Restricted Content on Discord*', accessed 16 Feb 2023, discord.com/safety/360043653552-age-restricted-content-on-discord; Discord, *'Age-restricted content and channels,* https://support.discord.com/hc/en-us/articles/115000084051-Age-Restricted-Channels-and-Content.

[798] Reddit, *'Content Policy',* https://www.redditinc.com/policies/content-policy

[799] Reddit, '*User Agreement'*, https://www.redditinc.com/policies/user-agreement-april-18-2023.

[800] Reddit, 'Content Policy'.

[801] Hive Moderation, *'Home page'*, https://hivemoderation.com/.

[802] Reddit, '*Moderator code of conduct*', 2022, https://www.redditinc.com/policies/moderator-code-of-conduct.

Other safety measures

In addition to industry's efforts to implement effective content moderation tools and processes, user empowerment features are vital complementary measures for preserving fundamental human, consumer, and digital rights.

User empowerment and autonomy tools give users the ability to customise and control their experiences on platforms. This can include permitting users mute certain words or content, or control who can contact them.

> Evidence from a 2021 UNICEF research report suggests that 'developing ground rules, providing tools for users to block and report problematic people and content, implementing technical solutions to minimize exposure to content risks, ensuring strong privacy settings by default and promoting user empowerment' are important considerations when building safety features into products and services.[803]

Throughout the consultation process, eSafety heard that many young people are unexpectedly seeing pornography on a variety of different services where they do not wish to see it. In this case, it is important for people to have tools to manage their own experiences.

Providing educational materials

Services can support user empowerment by including easy-to-understand information which educates users and can also motivate positive individual and group behaviour. For children and young people, providing incentivised and graduated experiences may assist in enhancing digital skills and fostering and sense of community. All layers of the **digital stack** have opportunities to proactively educate their users on online safety issues**.**

> **Optus** provides a Family Hub with information about a range of online, safety, privacy and security issues. This includes information about its Digital Thumbprint program, through which Optus delivers workshops to young people and families on online safety.
>
> **Vodafone and TPG** both also have information pages on their websites for users and for parents. This includes information about protecting your child online and using Family Friendly Filters.

[803] UNESCO, '*Digital Age Assurance, Age Verification Tools and Children's Rights Online across the Globe: A Discussion Paper'*, 2021, p.50.

Mozilla offers a Tech Talk resource to support Firefox users to talk to their children about a range of potential online harms, including access to pornography.[804]

Nudges and prompts

Services can motivate positive individual and group behaviour by implementing commendations, community endorsements, rewards, prompts, nudges, and reminders. Prompts, nudges, and reminders can be language or content-based and can educate users about what is acceptable and appropriate. Nudges could be applied to platforms which allow adult content to prompt users to apply appropriate tagging (enabling the use of blurring or removing it from children's feeds). For platforms which do not allow such content, nudges could remind users of the terms and conditions of the platform and prompt consideration on whether they want post the content.

Reporting mechanisms

Easy to use reporting mechanisms are essential to keeping users safe. Services have a responsibility to implement infrastructure that supports internal and external triaging, clear escalation paths and reporting on all user safety concerns, alongside readily accessible mechanisms for users to report concerns and violations at the point that they occur.

Ideally, reporting mechanisms should be available to users across all forms of a service – in-app, in-video and in real time, to ensure users can report content quickly.

Key reporting features a platform should consider are:

- Internal and external triaging
- Real time flagging of content for review
- Direct reporting on all types of accounts, content, activities and features
- Clear escalation paths and reporting on all user safety concerns
- Accessible and localised information about third party referral services

[804] Mozilla, *'The Tech Talk',* n.d., https://www.mozilla.org/en-US/firefox/family/.

Enabling user choice and control – preventing unintentional access to content

Services should consider policies and settings which empower and support users to have the experience that they expect online. This can be done through a range of methods and is specific to the platform or service and its users.

- In March 2022, **Google** announced it was using advanced AI technologies to improve its understanding of whether searches are truly seeking out explicit content, helping to reduce a user's chances of encountering these results by surprise. 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.[805]
- **xHamster**, a popular pornography site, enables users who have watched 10 or more videos to reset their recommendations.[806] This clears a person's viewing history, reducing the potential for unwanted content silos or filter bubbles. eSafety notes that this doesn't address concerns that algorithms show potentially harmful content to fresh users.
- **Instagram**, a social media service which does not allow nudity or 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 explicit. The Instagram help centre notes that the sensitive content control may not appear in settings for users who are under 18, presumably because the default setting is for sensitive content not to be recommended to those accounts.[807]

Stakeholders noted that the local adult industry takes steps to prevent children and adult users from unintentionally viewing their content, including:

- **Home or index page warnings** indicating the site contains adult content, so users do not stumble upon it by surprise (in addition to the RTA tagging discussed earlier)

[805] Google, '*Using AI to keep Google Search safe',* 2022, https://blog.google/products/search/using-ai-keep-google-search-safe/.
[806] xHamster, '*How to reset recommendations on xHamster*', xhamster.com/blog/posts/10331613.
[807] Instagram, *'Help Center: How to limit sensitive content that you see on Instagram'*, https://help.instagram.com/251027992727268.

- **Paywalls**, which increase friction and help create barriers that prevent children from accessing online pornography. Generally, credit card details are required to access content (as individuals must be at least 18 years old to apply for a credit card).
- Features to **prevent content from being downloaded** and shared outside the protection of the paywall and banning users who do share content elsewhere.

Conclusion

Services must use a suite of tools to keep children safe. They must constantly engage with communities as well as continually and proactively review those tools to ensure that they meet the evolving needs of their users and continue to be fit for purpose.

There are many available for creating safer user experiences. None of these tools or measures constitute a complete solution if used alone, they need to be deployed in tandem to be effective. By having a variety of interventions available, services can respond proportionately to the level of risk of children accessing age-inappropriate content in different contexts.

Chapter 12: Opportunities for change

Key points

- While technology is continuing to develop and improve, industry should be looking at best practice and collaboration across the digital ecosystem to collectively uplift safety outcomes for all users.
- Safety By Design encourages industry to proactively address harms which may occur, rather than retrospectively addressing harms after they occur. eSafety's Safety By Design principles, assessment tools and guidance material can supplement industry-led efforts to better understand and bolster safeguards to ensure age-appropriate design and prevent access to potentially harmful content and activity.
- eSafety has identified broad areas and opportunities for improvement for industry to consider:
    - using effective age assurance measures to create age-appropriate experiences.
    - tailoring safety measures and settings to reflect the evolving capacities of children.
    - improving the availability, accessibility and awareness of safety tools and settings
    - increasing policy clarity and improving enforcement practices
    - better supporting user control and choice
    - leveraging all participants in the digital ecosystem to improve outcomes and avoid unintended consequences.

Overview

There is a significant opportunity for industry to take further steps in preventing children's access to online pornography and to create better and safer experiences for all their users.

While many services (see chapters 8 and 11) have taken steps in recent years to implement age assurance and complementary measures to protect users and provide safe and age-appropriate experiences, significant gaps remain.

Aligned with the principles of Safety by Design, the online industry should put user safety and rights at the centre of the design and development of their online products and services. Beyond providers of digital platforms and services – other players in in the industry, including enabling and ancillary services providers, can play a role in encouraging the development and implementation of safer practices.

Reflecting on chapters 8 and 11, this chapter outlines lessons, opportunities and consideration for all participants in the digital ecosystem, as well as ancillary services, governments and other stakeholders.

Safety By Design

eSafety supports industry to create a safer and more inclusive digital ecosystem, particularly for those most at risk of harm, through our Safety by Design initiative.[808]

Safety by Design

Safety by Design encourages industry to anticipate potential harms and implement risk-mitigation and transparency measures throughout the design, development and deployment of a product or service. This approach seeks to proactively address harms which may occur, rather than retrospectively addressing harms after they occur. The following principles can be used by industry to support policy and service improvement measures to provide children with age-appropriate online experiences (including preventing encounters with online pornography).

Safety by Design principles

The initiative promotes online safety through three guiding principles:

[808] eSafety Commissioner, '*Safety by Design: Assessment tools*', eSafety website, n.d., https://www.esafety.gov.au/industry/safety-by-design/assessment-tools.

- **Service provider responsibility – the burden of safety should never fall solely upon the user.** Services should made sure online harms are understood, assessed and addressed in the design and provision of online platforms and services.
- **User empowerment and autonomy – the dignity of users is of central importance.** Products and services should align with the best interests of users as set out in chapter 4. This should be informed by consultation with the diverse user community of a product or service.
- **Transparency and accountability – these are hallmarks of a robust approach to safety.** They not online provide assurances that platforms and services are operating according to their published safety objectives and legal obligations, but also assist in educating and empowering users about steps they can take to address safety concerns.[809]

Until recently, the field of trust and safety was limited and not as developed as other long-standing disciplines, such as cybersecurity. This is changing, with many services integrating safety considerations as a strategic advantage for the long-term growth and health of their business.[810]

eSafety's Safety by Design resources and guidance materials (including risk assessment tools) can supplement industry-led efforts to better understand and bolster safeguards to ensure age-appropriate design and prevent access to potentially harmful content and activity.

Safety by Design assessment tools

eSafety has resources that support industry in making the Safety by Design principles actionable and achievable.[811] The tools guide and support technology companies to assess risks up front, and embed safety into the culture, ethos, and operations of their businesses. They are freely available on eSafety's website and can be optimised for both start-up and enterprise video streaming services, social networking services, entertainment sites, and other online services whose users may be adults, young people, and children. The current suite of resources intended to apply to a wide range of online services, including social media, dating platforms, and gaming and virtual communities.

[809] eSafety, '*Safety by Design: Principles and background*', n.d., https://www.esafety.gov.au/industry/safety-by-design/principles-and-background.
[810] Ipsos, '*Cyber Security Breaches Survey 2022'*, p3, 2022, https://www.ipsos.com/en-uk/cyber-security-breaches-survey-2022.
[811] eSafety, *'Safety by Design: Assessment tools*', n.d., https://www.esafety.gov.au/industry/safety-by-design/assessment-tools.

Lessons, opportunities and future considerations for the online industry

Through the exploration of existing and emerging measures, policies and tools in chapters 8 and 11, eSafety has identified several areas for improvement across the digital ecosystem to prevent and mitigate harms from children's access to online pornography and promoting their best interests. These lessons and opportunities and are not presented as recommendations, but as considerations for services to deliberate while reflecting on their particular circumstances, risk factors and user base. These suggestions for better practice may also be relevant considerations for future industry codes related to class 2 material.

Effective age assurance technologies at sign up and age detection tools to support users to have age-appropriate experiences

Many services are investing in methods to determine user ages and are continuing to develop new and innovative age assessment methods. Services should consider which methods are best suited to their platform, users, and unique safety risks and concerns.

Age assurance tools work most effectively when supplemented with complementary measures to create age-appropriate experiences. Correspondingly, complementary measures are most effective when services have an accurate understanding of users ages.

All participants in the digital ecosystem should consider where and how age assurance can be built-in. For example, if implemented at a device level, the device could share an age attribute (over-13 or over-18) with apps, browsers or websites. This could reduce the need for users to verify their age with each platform they use. It could also enable the effective use of other safety tools, such as age-tailored filters, settings and accounts. eSafety does not recommend the use of one form of age assurance over the other. As outlined in chapter 8, there are range benefits and risks to these technologies, including privacy and data collection concerns.

Safety tools and complementary measures should consider children's evolving capacities

Consultation stakeholders frequently raised concerns with the 'all-or-nothing' nature of some safety tools, such as parental controls and filters. There was also a perception that tools are likely to over-block, and subsequently censor, content. In research from the UK, 18% of parents of 12–17-year-olds said they didn't use parental controls and filters because they block too much or get in the way.[812] Tools of this nature might be appropriate for very young children,

[812] Ofcom, *Children's media use and attitudes*, 2022.

where providing a more controlled experience is necessary. However, these tools may not provide appropriate scope for children to exercise their rights to information, freedom and privacy as they get older.

Children of all ages deserve protection and safety, however the methods of providing safe and age-appropriate online experiences change as children they get older and acquire knowledge, competencies, and agency. Providing graduated stage- and age-based safety settings, means measures are more targeted in addressing the various risks and harms associated with access to online pornography while balancing children's digital rights. In our consultations, stakeholders raised the following graduated settings:

- Adaptive school-based filters which provide different experiences depending on year group or developmental stage.
- Social media platforms providing age-appropriate recommended content feeds for child users between 13-17 years of age, rather than providing all child users with the same experience.
- Younger device users may also benefit from more stringent privacy and safety settings, such as preventing contact from unknown users and limiting content sharing.

Opt-out age for parental controls

Some stakeholders we consulted with were critical of Google and Apple's policies to allow children aged 13 to opt out of device safety settings, while other expressed reservations on giving parents and carers full control of the information their teenage children could engage with online.

According to a report from C3P, 13–17-year-olds on Google Play were restricted in what apps they were able to view, access or download. For Apple's App Store, users were able to view and download apps that were rated 17+ or 18+, meaning once a child turns 13, they would no longer require parental permission to download apps via the Apple App store that are intended for adult users.[813]

If parents and children are finding that parental controls are no longer relevant, or are less useful as a child ages, providing more customisable settings and experiences may allow for more exploration and independence for a child while not completely removing safety measures.

[813] Canadian Centre for Child Protection, *'Reviewing the Enforcement of App Age Ratings in Apple's App Store and Google Play'*, 2022, https://www.cybertip.ca/pdfs/C3P_AppAgeRatingReport_en.pdf

Further consideration on opt-out ages should consider the children's privacy outcomes stemming from the government's response to the Privacy Act review report.

Improving the availability, accessibility and awareness of filters, parental controls and other tools

eSafety's consultations and review of available research highlighted concerns regarding the availability and accessibility of parental controls, filters and other tools, and limited parental awareness of these tools and how to use them.

Default settings

While many devices and services provide safety tools for their users, having tools turned on by default may be a more proactive and effect method to prevent the harms associated with online pornography. This may also assist with greater parental awareness and uptake of these tools.

For example, account-based safety and privacy settings on platforms, services, and devices could be set at the highest and most secure level when creating an account, with users able to adjust those settings as appropriate.[814] Default settings could also be tailored to a user's age – with youngest users having the strictest controls in place.

Additionally, when users attempt to change or update their default settings, prompts should be provided in plain language so that users understand the implications of any changes being made.

Consultation stakeholders discussed the benefits and challenges of opt in versus opt out safety features more broadly, including the need to ensure such features respected cultural diversity and varying individual levels of digital literacy. They also suggested that default settings do not replace the need for families to have discussions about expectations and boundaries for being online. Further discussion on the role of education and parents is at chapter 13.

While individuals may opt out of tools such as filters, having these tools on by default means users are empowered to control their online experience. Default settings also reduce the risk of users encountering unwanted content unintentionally (such as pornography) and could also result in fewer children being able to access online pornography in common spaces using public Wi-Fi.

[814] Robust and restrictive default privacy and safety settings for children is an example of reasonable steps that a service can take to ensure its safe use under the Basic Online Safety Expectations. Further consideration in chapter 14.

Improving the availability of built-in safety tools and parental controls (as opposed to paid third-party tools) could help to address other barriers to use such as cost.

Improving awareness of safety tools and increasing the digital literacy of users

A specific need identified in roadmap submissions and consultations was education and information for parents and carers about how to access and apply safety technology and tools.

Safety tool awareness raising

The approach taken by the Family Friendly Filter scheme of testing products and classifying them according to age segments has great potential to address previously identified needs to adjust safety settings over time as a child grows and develops. 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.

Services can support user empowerment by including easy-to-understand information about how to use available safety tools and measures on their devices or services. This information could be shared proactively – through partnerships with NGOs and facilitating parent-led, peer-to-peer education and information sharing. It could also be co-developed with, supported by and amplified by others, including governments. For example, 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.[815]

Other ways that industry can share best practice safety information with users:

- Prompts and nudges based on user behaviour – such as reminding users of service terms and conditions before they post content that may breach those terms.
- Providing information about the availability safety tools at sign up or when setting up a new device.
- Offering easy to understand information about the implications of accessing new settings/functions or related safety tools. For example, services could remind users about how to block or mute other users the first time they publicly share a post.
- Establishing an easily accessible and prominently displayed safety/privacy hub. This could also include specific sections for parents broke up into different age groups (for example, under 13s, 13-15 and 15-17).

[815] eSafety Commissioner, *'Gift Guide',* n.d., https://www.esafety.gov.au/parents/resources/gift-guide.

Greater knowledge and uptake of parental controls and filters should be also considered by government to improve the digital literacy of Australians.

Other barriers to uptake

While limited digital literacy and low awareness of these tools is a challenge – some stakeholders also pointed to other barriers, such as cost and ease of implementation. Further research could be considered to understand the extent of cost as a barrier to using filters and parental controls.

As noted, parental controls and safety tools should be easy to use – this should include guidance in a range of languages and consideration of different cultural contexts.

Increasing policy clarity and improving enforcement practices

While industry can set policies for creating safer experiences, it is important this is followed up with effective, transparent and consistent application of these policies.

Beyond the application of safety measures at an individual service level, peak bodies also have a role in building members' understanding and capacity for applying these measures across local industry. For example, Eros Association has developed guidance to assist the local adult industry in complying with the *Online Safety Act 2021* (Cth).

Policies relating to pornography and enforcement of those policies

Industry should have clear policies relating to online pornography, and transparent practices in the enforcement of those policies. This is an expectation on services under the Basic Online Safety Expectations for Social Media Services, Designated Internet Services and Relevant Electronic Services.

Policy enforcement

eSafety acknowledges that decisions about whether certain content breaches terms of service and or is inappropriate for children are affected by several factors, including decision-maker bias (human or algorithm).

Consultation participants from the domestic adult industry told eSafety that they often find it challenging to engage with social media companies regarding adult content policies. They reported receiving no advance warning for changes to Terms of Service or the way moderation policies were applied to content. They also felt that there was limited means for reviewing decisions. Policy enforcement should have appropriate and accessible appeals processes and be continuously improved in consultation with user communities.

Better policy calibration and content moderation practices for distinguishing between pornography and sexual health information can also support access to sexual health education materials, which can be important to a child's development.

Government, NGOs and academia could provide support and advice to the online industry on improving policies and enforcement practices regarding online pornography and age-appropriate experiences for users.

Minimum age policies and enforcing age requirements

eSafety research identified that children are seeing online pornography before the age of 13 (the minimum age for joining most social media websites) and are also seeing pornography on social media services.[816]

It is also common for children to sign up to social media sites before they turn 13 – using false birthdates or other means.[817] In addition to breaching the terms of service of many platforms, this can cause further issues over time – such as impacting the ability to provide age appropriate experiences and privacy settings. This speaks to the importance of effective age detection tools being in place.

Some services are detecting and removing underage users on platforms – TikTok's January-March 2023 transparency report stated that it removed 16,947,484 accounts suspected to be users under the age of 13 during that period.[818] However, there is a lack of transparency and consistency across the industry about what measures are being used and how effective they are. The minimum age for services should be clearly communicated to users, and effectively enforced.

Minimum age requirements and app stores

The role of app distribution services as gatekeepers to accessing apps means they can provide meaningful safeguards around the apps children can access. However, there is a lack of transparency in the criteria used to determine app age ratings.

Currently, age ratings given by the app distribution services are not well enforced, with users over 13 able to download apps that may have age ratings exceed their own age.[819] In addition, when setting up an account to use Google Play or Apple's App Store, users are required to

[816] eSafety, forthcoming research.

[817] Ofcom, '*Children's Online User Ages Quantitative Research Study*', 2022; eSafety Commissioner, '*The digital lives of Aussie teens*', 2020, https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf.

[818] TikTok, '*Community Guidelines Enforcement Report*', 20 June 2023, available at: https://www.tiktok.com/transparency/en-au/community-guidelines-enforcement-2023-1/.

[819] Canadian Centre for Child Protection, *'Reviewing the Enforcement of App Age Ratings in Apple's App Store and Google Play'*, 2022.

provide their date of birth. This may lead users to infer that devices enforce age ratings. This is not the case.

The default minimum age set by the app can differ from the age rating assigned by the app distribution service. For example, Discord, Reddit and Twitter permit users aged 13 and up to create accounts, but these apps are rated 17+ by the Apple App Store due to the nature of the content they permit on their service. However, users under 17 are still able to download these apps through the Apple App Store. Consultation participants discussed ways to encourage compliance by young people with age-restricted services. This included providing incentives or designing exclusive features for accounts with verified ages.

There is an opportunity for further engagement and consultation with young people to develop age-appropriate experiences that encourage them to provide accurate age information to platforms and not seek to circumvent age restrictions.

Better supporting user control and choice

Using recommender algorithms to support users in controlling their experience

As reflected in eSafety's position paper on recommender systems and algorithms, industry has many options available to it for mitigating harms (which include age-inappropriate material being recommended to children or systems serving increasingly harmful material based on user engagement):

- Recommender algorithms can help to curate age-appropriate experiences for younger users, by not promoting adult content to children, or to other users who have opted out from seeing such content. This can be helpful for a range of content types where viewer discretion is advised.
- Transparency around how service recommender systems determine recommended content could provide users with greater choice and control. Transparent practices can inform feedback loops which allow users input into what content they are recommended.
- Human review should be introduced when context is critical to whether content breaches terms of service or community guidelines.
- Services should apply proactive content moderation tools which trigger warnings or blurring for relevant content.
- Services should enable their user community to tag content for review. This can also be an effective way to help users avoid content they do not wish to see. As discussed below, users must be educated by platforms on the terms of service and community guidelines, as well as appropriate use of moderation tools to ensure these functions are used effectively.

- Affected stakeholders should be consulted to make sure warnings and labels are appropriate. Where content warnings are provided to some users and not others, consideration should be given to the data which informs these choices and the risk of bias. For example, a system calibrated to deprioritise sexually explicit content may inadvertently remove sexual health content from recommendations, making it difficult for users to find valuable information. Interventions such as downranking are harder to measure and are less transparent than content removals.

Informing users and preventing inadvertent access to pornography

> ‘I would like them [young people] to be able to feel good about it [seeing pornography], because the only time they'd see it is if they WANTED to see it, and looked for it, rather than it being shoved into their faces by strangers.’ – eSafety focus group participant, 18

Unintentional viewing of pornography was frequently reported in our primary research. This points to improvements services can make in identifying content that breaches terms of service, or creating design experiences which support users to avoid unexpected or unwanted explicit content.

eSafety noted that only one of the top 5 most visited pornography sites in Australia had any form of age gate or pop-up warning users on their first visit that the site contained pornography, offering users a chance to exit before viewing any content. Introducing friction can add to barriers preventing children from viewing online pornography, especially unintentionally.

It is also beneficial for all users to be informed of, and consent to, viewing online pornography. For services where the primary purpose is providing online pornography this can include having home page warnings that inform visitors of the website’s pornographic content, designing landing pages to exclude explicit content, disenabling content auto-play, and at a minimum requiring users to enter an age gate and actively opt-in to viewing content. Content that is behind a paywall, reported as common practice by the domestic adult industry, also generates friction.

While these measures are not foolproof – and will not prevent motivated individuals from seeking to circumvent these measures – they represent an improvement from current practice. For services which host explicit and non-explicit content – the provision and enforcement of clear policies for applying sensitive tags or labels, content warnings and allowing users to opt-in or out of viewing such content (based on age or for adults, preference) also addresses issues of unintentional access.

Respecting the autonomy and expectations of users is an important element of designing safe experiences and should be considered by all participants in the digital ecosystem.

Leveraging networks and relationships across the digital ecosystem

Industry should consider the opportunities for leveraging different parts of the ecosystem to encourage better safety outcomes overall but should also identify any unintended consequences from these measures. Cooperation between layers of the digital stack and a whole of ecosystem approach could mitigate some of these concerns. In addition to regulatory requirements imposed by governments, others with influence over digital ecosystem actors can encourage or require more robust safety measures.

Investors

Venture capital (VC) funds and investors provide key financial support to industry, including growing early-stage technology companies and can have the ability to shape processes and company structures.

Online services focused on user safety, which implement robust age assurance processes, could see an increased level of brand protection, mitigating potential risks to their reputation and revenue, making them safer, more attractive investment opportunities.[820] Alternatively, if penalties for failing to prevent children's access to harmful content are insubstantial, a company and its shareholders may elect to pay those costs rather than investing in robust age assurance and safety processes.

Requirements for using age assurance technologies would likely generate interest from the investment community looking to capitalise on market uplift and meet the goals of corporate environmental, social and governance (ESG) practices and funds.[821]

eSafety's Safety by Design initiative encourages investors and the venture capital community to take a leading role in making sure technology companies put safety and ethical considerations at the heart of their design processes. It includes an investor checklist to help assess a company's capacity for managing online safety risks. It also contains a set of model clauses for due diligence, which can be adapted to make sure online safety considerations are built into investments. Access to illegal and harmful content is one of the areas raised in these resources and an early-stage technology company could consider implementing age assurance, among other complementary safety measures, to reassure investors and shareholders that user safety is a priority.

[820] Ipsos, '*Trust, Safety and the Digital Economy*', p13, 2022, https://www.ipsos.com/en-uk/trust-safety-and-digital-economy.

[821] ESG is often synonymous with Corporate Social Responsibility (CSR) and Socially Responsible Investments (SRI).

Advertisers

Advertising

The Australian Association of National Advertisers' (AANA) Children's Advertising Code states that advertising or marketing to children must not employ sexual appeal or include sexual imagery.[822] However, despite digital marketers' ability to collect and use data to deliver highly personalised and targeted ads, there is evidence that children are receiving advertising for age-inappropriate products and services.[823] In our research, 28% of participants aged 16-18 reported seeing online pornography ads on social media. In addition, while the Code of Ethics bans overtly sexual images from being shown in physical environments where children are likely to encounter them,[824] it does not account for the digital environment.

Further action could be taken by the advertising industry to make sure their pledge to keep harmful or inappropriate advertising away from children in the offline world is matched online.

Advertising is a predominantly self-regulated field,[825] with guidelines and codes established by peak bodies and industry representative organisations. The Global Alliance for Responsible Media (GARM) has produced several frameworks and reports that provide guidance to marketers, media buying agencies, and digital platforms. This includes an Aggregated Measurement Report, allowing advertisers to see how well selected digital platforms are aligning to four key areas:

- How safe is the platform for consumers?
- How safe is the platform for advertisers?
- How effective is the platform at enforcing its safety policy?
- How responsive is the platform at correcting mistakes?[826]

[822] Australian Association of National Advertisers' (AANA), '*Children's Advertising Code'*, 2021, https://aana.com.au/wp-content/uploads/2022/06/AANA_Advertising_Code_for_Childrens_V2.pdf.
[823] ACCC, '*Digital advertising services Inquiry: Final report*', ACCC website, 2021, https://www.accc.gov.au/system/files/Digital advertising services inquiry - final report.pdf.
[824] AANA, *'Code of Ethics: Practice Note'*, AANA website, 2021, https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_PracticeNote_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=ethics-notes.
[825] Ad Standards, '*Advertising self-regulation'*, n.d., https://adstandards.com.au/about/self-regulation
[826] World Federation of Advertisers, '*GARM Aggregated Measurement Report Vol. 4*', WFA website, 2022, https://wfanet.org/leadership/garm/about-garm.

The November 2022 measurement report shows that 'Adult and Explicit Sexual Content' is a key focus area for all participating platforms. Issues relating to GARM's Adult and Explicit category were the primary reasons for removal during the relevant reporting period for YouTube, Pinterest, and Snap.[827]

By encouraging greater transparency and accountability by digital platforms, advertisers can promote an environment where digital platforms compete for advertising dollars by showing the proactive steps they are taking provide safe and age appropriate user experiences.

Payment processors

Where an online service relies on payment processors to enable users to purchase content, payment providers can exert influence through their policies on what purchases they will facilitate and any restrictions they impose. Payment providers have a variety of policies in relation to pornography. For example, PayPal's acceptable use policy prohibits use of PayPal for 'certain sexually oriented materials or services,'[828] and Stripe prohibits its use for adult content and services.[829]

Typically, pornography services offering paid content must work within the policies of banks and **payment gateways**, which in turn, must comply with payment processor conditions. Mastercard, has a Business Risk Assessment and Mitigation initiative which is designed to protect Mastercard and its customers from illegal and brand-damaging transactions.'[830]

In recent years, there have been some prominent examples of payment processors' influence in this space. For a brief period in 2021, OnlyFans announced plans to ban explicit sexual content on the basis that banks would not work with OnlyFans due to its reputation for hosting pornography.[831] Visa and Mastercard also announced they would suspend payments for advertising purchases on Pornhub after media reports alleged that child sexual exploitation material was hosted on the website.[832]

Consultation stakeholders raised opportunities and risks in involving payment processors in compliance. Some believed this would be a highly effective lever to secure compliance from services that might otherwise ignore jurisdiction-specific regulatory requirements. Others,

[827] World Federation of Advertisers, GARM Aggregated Measurement Report Vol. 4.
[828] PayPal*, 'PayPal Acceptable Use Policy'*, Paypal website, 2021, https://www.paypal.com/va/webapps/mpp/ua/acceptableuse-full.
[829] Stripe, '*Prohibited and Restricted Businesses*', Stripe website, 2022, https://stripe.com/au/legal/restricted-businesses.
[830] Mastercard, '*See how our rules can help inform and guide your business*', n.d., https://www.mastercard.us/en-us/business/overview/support/rules.html.
[831] A Robertson, *'The payments mess that almost scared OnlyFans away from sex work: When playing for porn gets complicated*', The Verge, 2021, https://www.theverge.com/2021/8/27/22641095/onlyfans-sex-work-ban-online-porn-payment-processing-controversy.
[832] M DeGeurin, '*Visa and Mastercard Suspend Pornhub Ad Payments Amid Child Abuse Material Lawsuit*', Gizmodo, 2022, https://www.gizmodo.com.au/2022/08/visa-and-mastercard-suspend-pornhub-ad-payments-amid-casm-lawsuit/.

particularly sex workers, believed the policies and decision-making processes of payment providers were opaque and unfair, especially given limited avenues to appeal decisions or contribute to policies.[833] Accordingly, they argued that any related enforcement measures should be accompanied by consultation, procedural fairness and review mechanisms.

ISP blocking

ISPs can play an important role in enforcing sites' compliance with legal and regulatory requirements. For example, in Australia, DNS blocking is undertaken by ISPs in response to court orders or regulatory notices in relation to copyright infringement,[834] illegal online gambling[835] and the availability of material promoting, inciting, instructing in or depicting 'abhorrent violent conduct' such as murder or rape which is likely to cause significant harm to the Australian community.[836] In other jurisdictions, such as France and Germany (see: chapter 10), ISPs can be required to block adult sites which fail to comply with age assurance requirements. While individuals and pornography sites can take steps to circumvent these measures, DNS blocking can reduce traffic to those sites, creating compliance incentives. Consultation stakeholders raised ISPs, device and operating system providers and browsers – as playing an important role in achieving compliance with age assurance measures.

Measures to promote children's best interests and right to safety must also be assessed against the impacts they have on other rights, including the right to freedom of information, opinion and expression.

Domain Administrators and Registrars

Domain administrators and registrars have an obligation to address Domain Name System (DNS) abuse. This is generally understood as including malware, botnets, phishing, pharming, spam, and may extend to security threats such as denial-of-service attacks or DNS cache poisoning, as well as child sexual exploitation and abuse.[837] It has not traditionally extended to non-compliance with legal or regulatory requirements in relation to restricting children's access to online pornography or other content. ICANN, the Internet Corporation for Assigned Names and Numbers[838], has taken the position that 'it is not the Internet content police'.[839]

[833] Appendix 5.
[834] R Chirgwin, '*Australian carriers ordered to block more pirate streamers*', February 2022, https://www.itnews.com.au/news/australian-carriers-ordered-to-block-more-pirate-streamers-576415.
[835] Australian Communications and Media Authority, '*Blocked gambling websites', n.d.,* https://www.acma.gov.au/blocked-gambling-websites.
[836] *Online Safety Act 2021* (Cth) Part 8.
[837] Verisign, '*Combating DNS Abuse*', n.d., https://www.verisign.com/en_US/company-information/dns-abuse/index.xhtml#:~:text=What%20is%20DNS%20Abuse%3F,other%20forms%20of%20DNS%20abuse.%22.
[838] ICANN, '*What Does ICANN Do?',* 2012, available at: https://www.icann.org/resources/pages/what-2012-02-25-en.
[839] A Grogan, '*ICANN Is Not the Internet Content Police*', https://www.icann.org/en/blogs/details/icann-is-not-the-internet-content-police-12-6-2015-en.

However, some registrars, such as Moniker, have included this issue in their anti-abuse policy:

> ‘The following areas may not necessarily constitute abuse, but may be treated as such unless they follow certain requirements:
>
> ...distribution of erotic or pornographic or otherwise sexually explicit content is only permitted in observance of the applicable legal requirements. For example, the use of any Service for publication or distribution of such content without sufficient age verification techniques (thereby allowing minors to view such content without appropriate barriers), as well as use in violation of the requirements and directives of the authorities or appropriate registration authorities, is strictly prohibited.’[840]

Incorporating this expectation into policy enables domain administrators and registrars to act against sites which fail to take reasonable steps to prevent children from encountering online pornography. Actions could include suspending domain names, notifying registrants of suspensions and providing a mechanism for dispute, reviewing other domains owned by registrants for similar issues, and notifying relevant web hosting providers so they can consider taking action under their own policies or terms of service.[841]

Administrators and registrars can also play a role in preventing and mitigating the registration of ‘mirror’ sites. These are duplicate sites created to circumvent regulatory or legal enforcement actions, such as blocking of illegal gambling sites or movie pirating sites. As discussed in chapter 10, this is also a tactic that has been employed by pornography sites subject to ISP blocking orders internationally. Registrars such as GoDaddy already offer services to customers to proactively block registration of corresponding domain names to help brands preserve their reputation; [842] similar measures could be applied to prevent regulatory circumvention and uphold the rule of law.

eSafety acknowledges concerns raised by digital rights advocacy organisations such as Article 19 and AccessNow about extending the concept of DNS abuse to include failure to moderate harmful content, and the consequences this has for rendering entire sites inaccessible.[843]

[840] Monikor, *‘Anti-abuse policy’,* n.d., https://www.moniker.com/legal/anti-abuse-policy .

[841] DNS Abuse institute*, ‘Compromised Sites and Malicious Registrations: Best Practices for the Identification and Mitigation of DNS Abuse’,* December 2021, https://dnsabuseinstitute.org/best-practices-identification-mitigation-of-dns-abuse/.

[842] GoDaddy, ‘*Domains Help’,* n.d., https://au.godaddy.com/help/about-adultblock-and-adultblock-40865.

[843] Article 19, ‘*Internet: Content moderation at infrastructure level puts rights at risk’*, Article 19 website, 25 October 2021, https://www.article19.org/resources/icann-content-moderation-at-the-infrastructure-level-is-a-dangerous-move/; Article 19, ‘*Online freedoms: Safeguards must be balanced with free expression*’, Article 19 website, 10 June 2021, https://www.article19.org/resources/online-freedoms-safeguards-must-be-balanced-with-free-expression/; AccessNow, ‘*26 recommendations on content governance: a guide for lawmakers, regulators, and company policy makers*’, March 2020, https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf.

Transparency, procedural safeguards and clear rules based on the principles of necessity and proportionality are critical.

Hosting services

Like domain administrators and registrars, hosting services can set expectations and terms of service for the sites they host which oblige them to take reasonable steps to prevent children's access to online pornography. Reflected Networks, a hosting services company, provides a set of Content Moderation Best Practices which it recommends to customers which allow adult content to be uploaded by users. These include:

> 'Only users who have verified their age and identity should be permitted to upload adult content on customers' sites. UGC Customers must ensure that all uploaders are over the age of 18 and must use industry-standard age and identity verification services.'[844]

If a hosting service becomes aware that a site it hosts is not meeting these expectations, it could provide the site with an opportunity to put in place appropriate measures or suspend its services.

Again, stakeholder concerns regarding infrastructure-level content moderation and regulatory action[845] are acknowledged and eSafety emphasises the importance of proportionality, transparency, and procedural safeguards in determining appropriate measures.

The role of hosting services in enforcing sites' regulatory compliance is already contemplated by the Online Safety Act, as noted in chapter 6. Consideration could be given to adjusting the scope of this power, as explained in chapter 14.

Search engines

In addition to taking steps to improve the safety of their own products and services, search engines can play an important role in incentivising regulatory compliance and improved safety measures among the sites they list in their search results.

Currently, the eSafety Commissioner can give a link deletion notice to a search engine in certain circumstances where the linked site has refused to comply with a removal notice.[846] Consideration could be given to adjusting the scope of this power, so it could be applied in

[844] Reflected Networks, '*Content Moderation Best Practices*', n.d. https://reflected.net/cmbp.php.
[845] Article 19, '*Internet: Content moderation at infrastructure level puts rights at risk*'; Article 19, '*Online freedoms: Safeguards must be balanced with free expression*'; AccessNow, '*26 recommendations on content governance: a guide for lawmakers, regulators, and company policy makers*', 2020.
[846] Online Safety Act 2021 (Cth), s 124.

circumstances where a site has repeatedly refused to comply with legal requirements and regulatory notices to prevent children's access to online pornography. Sites may be more inclined to comply if their failure to do so could result in reduced search traffic and revenue.

Addressing unintended consequences across the ecosystem

As noted above stakeholders noted that measures which create too much friction have the potential to deter users from accessing compliant site - people may simply leave a site or service if they are uncomfortable with the age assurance measures it applies and try to find the content somewhere else. 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. Stakeholders noted that this would likely also impact search engine rankings. It is important then that search engines are participants in these efforts and consider child safety measures in their ranking algorithms to avoid promoting harmful content.

Conclusion

eSafety's qualitative research found that for most young people, choice is key when it comes to online pornography. Young people in our focus groups discussed their right to safe, autonomous sexual development and exploration – which included for some, choosing not to see online pornography. Services should consider the safety of their users as central to their design and provide them with the tools and frameworks to experience the online world safely.

The discussion in this chapter highlights a range of possible measures or steps towards better practice within industry to enhance the safety of children regarding access to online pornography. There is a role for all sections of the online industry in supporting children's best interests online. This could be through the implementation of measures or tools to create safer experiences, or by leveraging influence across the digital ecosystem.

Areas of consideration for better practice:

- Ensuring the use of effective age assurance technologies at sign up and age detection tools to support users to have age-appropriate experiences.
- Designing and implementing safety tools and complementary measures that consider and reflect children's evolving capacity
- Improving the availability, accessibility and awareness of safety technology
- Increasing policy clarity and improving enforcement practices
- Providing measures and tools that support users choices and provide them with control over their experiences

The table presents a summary of possible actions outlined throughout chapters 8, 11 and 12 that the online industry could undertake improve user safety, empowerment and autonomy in the context of access to online pornography.

Children’s access to online pornography is a complicated issue which needs a nuanced and layered response. Different services will need to consider how potential actions suit their particular platform, userbase, risk factors and existing rules and policies.

Summary table of considerations for the online industry to restrict children's access to pornography

			Age Assurance	Age-appropriate settings	Complementary measures	Transparent and consistent policies	Tools for user choice and control	Leveraging
Subject to Industry Codes	Subject to the Basic Online Safety Expectations	**Social Media Services**	Consider how age assurance or age verification tech can be built in in a way that's best suited to their platform, users, and unique safety risks. Reasonable efforts to measures to detect and deter under-age users	Create child accounts and tailor experiences for younger users.	Having safety and privacy settings turned on by default. Providing clear sources of safety information for users. Prompts and nudges based on user behaviour.	Minimum age for services should be clearly communicated and effectively enforced. Consult on, implement and enforce clear policies on what content is allowed. Include accessible appeals processes.	Providing transparency and user input into recommender systems. Allowing users to opt in or out for certain types of content. Consider different pathways for content moderation – including blurring. Enable and encourage accurate user tagging or labelling of content.	-
		Relevant Electronic Services	Age gates and reasonable efforts to detect and deter under-age users	Create child accounts and tailor experiences for younger users	Prompts and nudges based on user behaviour	Minimum age for services should be clearly communicated and effectively enforced. Consult on, implement and enforce clear policies on what content is allowed. Include accessible appeals processes.	-	-
		Designated Internet Services	Age gates and reasonable efforts to detect and deter under-age users (including the use of paywalls).	-	Online safety information, content warnings. Use of metatags and other methods to ensure content is able to be blocked by parental controls and other filters.	Minimum age for services should be clearly communicated and effectively enforced. Consult on, implement and enforce clear policies on what content is allowed. Include accessible appeals processes.	Where hosting pornography: Introduce a landing page or home page warning for visitors and require them to click through to access content. Disable auto-play. Enable and encourage accurate user tagging of content.	
		Devices (including OS)	Consider on-device age assurance and sharing of age attribute	Tailor experiences for younger users and provide more options as users age.	-	-	-	-
		App distribution services	-	Tailor experiences for younger users and provide more options as users age.	-	Consistent age ratings, Enforce existing policies against sexually explicit content Include accessible appeals processes.	-	Encourage compliance of apps through enforcing existing policies.
		ISP	-	-	Make safety information available	-	-	Encourage compliance
		Hosting Services	-	-	-	Consult on, implement and enforce clear policies on what content is allowed. Include accessible appeals processes.	-	Develop and enforce policies encouraging services to comply with requirements to take reasonable steps to ensure children aren't able to access pornography. Provide mechanism for appeals.
		Search Engines	-	-	Enabling safe search options and safe features	-	-	Ensure compliant sites aren't penalised in rankings
		DNS	-	-	-	-	-	Develop and enforce policies encouraging services to comply with requirements to take reasonable steps to ensure children aren't able to access pornography. Provide mechanism for appeals. Take mitigating actions to prevent the registration of mirror sites
		Industry/Industry Organisations	-	-	Make safety information available	-	-	Encourage compliance
		Safety Tech Sector	-	Provide options in tools to reflect the evolving capacities of children.	Make safety information available	-	-	-
		Browsers	-	Enabling safe browsing settings	Support for safety technology integration	-	-	-
		Investors and shareholders	-	-	-	-	-	Encourage compliance
		Advertisers	-	-	-	Take action to ensure online ads meet same standards as offline ads in not targeting children with adult content	-	Encourage compliance
		Payment providers	-	-	-	Consult on, implement and enforce clear policies.	-	Encourage compliance

eSafety next steps and recommendations for the Australian Government

eSafety next steps

- The findings of the research, consultations and the independent technical assessment set out in this part will inform several of eSafety's workstreams.
- In addition, the good practices, gaps and overall analysis of age assurance technologies will inform the development of the next phase of industry codes or standards, as discussed in chapter 14.
- eSafety will also make sure guidance produced to support online service providers in complying with the Basic Online Safety Expectations (see chapter 14) is informed by this report's analysis of age assurance technologies.
- We will continue issuing reporting notices to online service providers to enhance their transparency and accountability in relation to the Basic Online Safety Expectations. 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 continue to collaborate across government on intersecting initiatives and reforms, such as the classification review, the Privacy Act Review, and digital identity developments.
- eSafety will continue to engage with its international counterparts, including the through Global Online Safety Regulators Network, to:
    - maintain an awareness of policy and legislative developments related to restricting children's access to online pornography and the uptake of online age assurance measures for age restricted goods and services.
    - continue to build an evidence base and learn from international pilots of age assurance technologies, as well as successes and challenges from internationally legislated technological measures to restrict children's access to pornography.
    - ensure any age assurance measures considered in Australia are harmonised and consistent with other jurisdictions where possible, to facilitate industry compliance and aid enforcement.

Safety by Design

- The findings of this report will Inform eSafety's engagement and sharing of good practice with the online Industry, Including 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.

Recommendations for the Australian Government

- Fund eSafety to:
    - 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.
    - 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.
- 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.
- 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
- Government should also consider the need for public awareness raising efforts to promote understanding of and trust in any age assurance pilot or mandate.

eSafety recommends the Australian Government consider the following arrangements in relation to a pilot

- **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. 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:** 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.

eSafety recommends the following cross-government stewardship arrangements for any future pilot initiative:

- 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 Commonwealth, State and Territory Data and Digital Ministers could also prove beneficial.

Part IV – How Australia can prevent and minimise harm through education and regulation

This volume of the report is focused on how the technological measures discussed in Part 3 can be mandated and enforced through regulation. It also outlines the educational measures which should accompany any technological response, to provide a holistic approach to harm prevention and mitigation.

Table of contents

Chapter 13: The role of education in protecting and empowering children

Key Points

- It is important to support children in understanding the content they encounter online, including online pornography in a manner that respects their evolving capacities. Trusted adults should have the necessary skills and knowledge to discuss online pornography with children.
- Any approach should consider the changing needs, rights, and best interests of children at different ages and stages.
- Some young people are critical of how sex and relationships education is delivered. Many see the value in inclusive, stigma-free education. Youth participation and co-design can help make sure messaging is relevant, relatable, authentic, and effective. It can also make sure the content meets young people's needs. This was reiterated by most stakeholders.
- There are several relevant areas of the curriculum where education on online pornography could be integrated but children should also have access to age appropriate resources they can explore independently.
- Education should allow for exploration of diverse perspectives in a constructive, trusting, and respectful way. There are many existing initiatives and good practice to build on in this space. There is also an array of new work commencing – particularly in the areas of consent, respectful relationships and prevention of gender-based violence – including as part of the National Plan to End Violence against Women and Children 2022-2032 (National Plan).
- Teachers, school wellbeing staff and other frontline workers often feel unprepared to talk about pornography with students. They need tailored materials to have safe and age-appropriate conversations.
- Government and industry can do more to raise awareness and educate people about existing and emerging safety tools.

Overview

Education plays an integral role in preventing and mitigating harms to children from online pornography. As children grow and evolve, so does the content and complexity of the issues taught. eSafety acknowledges the importance of a scaffolded approach to online safety education from the early years through to the secondary school years. This approach includes equipping schools, families, and external education providers to support children and young people as they navigate their way through the various challenges of the online world.

eSafety provides national leadership in raising awareness about online safety issues through audience-specific and evidence-based advice, content, and programs that give all Australians the skills and confidence they need to have safer online experiences. eSafety's legislated functions include supporting, encouraging, conducting, accrediting and evaluating educational, promotional and community awareness programs that are relevant to online safety for Australians.[848]

As part of the roadmap, eSafety was asked to consider activities for awareness raising and education, as well as complementary measures to make sure age verification is part of a broader, holistic approach to addressing risks and harms associated with children's access to online pornography.

eSafety has an existing body of foundational work covering good practice in online safety education which can support the roadmap.[849] In addition, a National Online Safety Education Coordination Council (Council) has been established to foster greater cooperation with Government, Catholic and Independent school education sectors in each state and territory. eSafety consulted the Council on the development of the roadmap at its first meeting in late 2022.

eSafety also consulted its community of endorsed providers, under the Trusted eSafety Provider Program,[850] to incorporate their expertise and insights into the roadmap. Lastly, eSafety has drawn on relevant projects funded through eSafety's Online Safety Grants Program[851], to identify practical and innovative education and training projects that can support children, young people and their communities to minimise harms to children from online pornography.

[848] Online Safety Act 2021 (Cth), s 27(f).
[849] eSafety Commissioner, *Best Practice Framework for Online Safety Education*, eSafety website, n.d., available at: https://www.esafety.gov.au/educators/best-practice-framework.
[850] eSafety Commissioner, *Trusted eSafety Providers*, eSafety website, n.d., available at: https://www.esafety.gov.au/educators/trusted-providers.
[851] The Online Safety Community Grants Program was announced as part of the First Action Plan 2022–2027, under the National Plan to End Violence against Women and Children 2022-2032. The program will support a range of projects that promote online safety for women and children. A total of $10 million will be made available over five years from 2022–23. See eSafety Commissioner, *Online Safety Grants Program*, eSafety website, n.d. Available at: https://www.esafety.gov.au/about-us/what-we-do/our-programs/online-safety-grants-program

The importance of education was highlighted throughout the research submitted to and conducted by eSafety, as well as in consultations held with all stakeholder groups – including children and young people themselves. They emphasised inclusive, evidence-based and stigma-free education about online pornography and the related topics of sexuality, consent and respectful relationships should be available to children and young people as well as the adults who support them to navigate the subject matter as they mature, including parents and carers, educators and frontline workers.

There were three main reasons education was seen as critical to efforts to prevent and mitigate risks and harms associated with children's access to online pornography. First, while there are many reasons children and young people seek out pornography, one is to learn about sex.[852] Children and young people have a right to safe, accurate and age-appropriate education and information about sex.[853] To reduce reliance on pornography as a learning guide, sexuality, consent and respectful relationships education needs to be updated to better capture pornography literacy, consent and guidance to prevent harm or injury because of physical intimacy.[854] Children and young people should also have access to other trustworthy sources of

[852] Our Watch, *Pornography, young people and preventing violence against women background paper*, 2020. Available at: https://www.Our Watch.org.au/resource/pornography-young-people-and-preventing-violence-against-women-background-paper-2020/; E Rothman et al., *'Without porn … I wouldn't know half the things I know now: A qualitative study of pornography use among a sample of urban, low-income, black and Hispanic youth*', The Journal of Sex Research, 2015, 52(7):736-746, DOI: 10.1080/00224499.2014.960908; K Dawson, S Nic Gabhainn and P MacNeela, *'Dissatisfaction with school sex education is not associated with using pornography for sexual information'*, Porn Studies, 2019; M Stoilova, S Livingstone and R Khazbak, *'Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes*,' in UNICEF Innocenti Discussion Paper 2020-03, 2021; E Rothman and A Adhia, '*Adolescent Pornography Use and Dating Violence among a Sample of Primarily Black and Hispanic, Urban-Residing, Underage Youth*,' Journal of Behavioural Sciences, 2016, 6(1). DOI:10.3390/bs601000; C Rosengard et al., '*Family Sources of Sexual Health Information, Primary Messages, and Sexual Behavior of At-risk, Urban Adolescents*,' American Journal of Health Education, 2012, 43(2):83–92, DOI:10.1080/19325037.2012.10599223; M Smith, '*Youth Viewing Sexually Explicit Material Online: Addressing the Elephant on the Screen*', Sexuality Research & Social Policy, 2013, 10(1):62–75, DOI:10.1007/s13178-012-0103-4; A Goldstein, '*Learner, laugher, lover, critic: young women's normative and emerging orientations towards pornography*,' Porn Studies, 2021.

[853] United Nations, *UN Convention on the Rights of the Child* (Articles 13 & 28), UN website, 1989, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child; International Women's Health Coalition*, The Human Rights of Children and their Sexual and Reproductive Health,* Centre for Reproductive Rights website, 2001, available at: https://reproductiverights.org/the-human-rights-of-children-and-their-sexual-and-reproductive-health/; United Nations Educational, Scientific and Cultural Organization (UNESCO), '*International Technical Guidance on Sexuality Education: An evidence-informed approach*', revised edition, Paris, France, 2018, available at: https://unesdoc.unes-co.org/ark:/48223/pf0000260770; A McKee et al., *'Healthy sexual development: A multidisciplinary framework for research'*, International Journal of Sexual Health, 2010, 22(1):14-19.

[854] Australian Association for Adolescent Health Ltd (AAAH), '*Comprehensive Sexuality Education in Schools: Position Paper, Australian Association for Adolescent Health, Australia*', 2018; K Litsou et al., *'Learning from pornography: results of a mixed methods systematic review*,' Sex Education, 2020, 21(2):236-252; K Dawson, S Nic Gabhainn and P MacNeela 2019; K Hare, J Gahagan and L Jackson, et al*., 'Revisualising 'porn': How Young Adults' Consumption of Sexually Explicit Movies Can Inform Approaches to Canadian Sexual Health Promotion*,' Culture, Health and Sexuality, 2015, 17(3):269-283; C Wright et al., *'Young people's needs and preferences for health resources focused on pornography and sharing of sexually explicit imagery*', Public Health Research & Practice, 2021, 31(1); M Crabbe and M Flood, *'School-Based Education to Address Pornography's Influence on Young People: A Proposed Practice Framework,' American Journal of Sexuality Education*', 2021, 1-46, DOI:10.1080/15546128.2020.1856744; P Ezer et al., *'School-based relationship and sexuality education: what has changed since the release of the Australian Curriculum?'*, Sex Education, 2020, 20(6):642-657; K Albury, *'Porn and participation: implications for learning and teaching practice'*, Porn Studies, 2018; P Byron et al., *'Reading for realness: Porn literacies, digital media, and young people*', Sexuality & Culture, 2021, 25(3):786-805; See Appendix 5; 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.

information on these topics which they can get independently or through services outside school.

> ‘I feel like education is the BIGGEST factor on how people feel about online porn. Those who don't get the right education either think it's completely wrong [for everyone to consume], or take it as the Bible [of sexual practice]’ - eSafety focus group participant, 18

Second, no age verification measure or other technological solution will ever be completely effective at preventing all children and young people in Australia from accessing online pornography until adulthood. Consequently, it is important to equip children and young people with the knowledge and skills to contextualise and critically interpret any material they do come across. This will build their capacity to determine the extent to which the material reflects the nature of real-world relationships and intimacy, aiding the mitigation of harms outlined in chapter 5.[855] In eSafety’s focus groups with young people, education was most often raised as a way young people could feel more equipped to navigate encounters with online pornography.

> ‘Yeah! just like how they teach safe sex in school they should teach safe use of online pornography. You will never be able to stop teenagers from using it so teaching them how to navigate it safely would benefit them.’ - eSafety focus group participant, 17
>
> ‘Maybe education on healthy sexual relationships so there is some reference point to viewing nsfw content and in deciding if it's too extreme’ - eSafety focus group participant, 18

Third, even if children and young people are prevented from accessing online pornography until adulthood, they are free to access it when they turn 18. In a 2018 survey conducted by eSafety, 69% of Australian parents and carers felt it is best to educate children and young people about online pornography because they will see it eventually.856 Further, the stakeholders we consulted felt that education which helps young people to contextualise what they see online is a key element of violence prevention.[857]

[855] L Vandenbosch and J van Oosten, *‘The Relationship Between Online Pornography and the Sexual Objectification of Women: The Attenuating Role of Porn Literacy Education*,’ Journal of Communication, 2017, 67(6):1015-1036; UNICEF, ‘*What works to prevent online and offline child sexual exploitation and abuse?’*, UNICEF website, 2020; C Wright et al., 2021; eSafety Commissioner, ‘*Summary of Call for Evidence on Age Verification’*, eSafety website, n.d, available at: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification#call-for-evidence; See Appendix 5.
[856] eSafety Commissioner, *Parenting and pornography summary report’*, p16, eSafety website, 2018, available at: https://www.esafety.gov.au/sites/default/files/2019-09/summary-report-parenting-and-pornography.pdf.
[857] See Appendix 5.

Within the research, the provision of robust sex and respectful relationships education, as well as social and emotional learning during childhood, has been linked to reductions in child sexual exploitation, abuse, and gender-based violence.[858] If developed and delivered effectively, such programs should serve to build resilience, resistance and emotional and digital literacy to counter harmful scripts about sexual violence that may be encountered in online pornography, including gender-based violence, hyper-sexualisation, and the objectification of women common in mainstream pornography.[859] It may also increase children and young people's capacity to have respectful and healthy attitudes towards women and respectful, consent-informed relationships into adulthood.[860]

This chapter explores current online pornography education for different audiences and age groups, identifies some of the relevant work already underway, and suggests areas where there may be gaps for eSafety and others to fill.

> '(In an ideal world, what would you like young people to think and feel if they see online porn?) To feel comfortable enough in themselves to make the right informed decision- whether that is to show a trusted adult, report it, or know what it is and move on with their day without too much discomfort but also not while being desensitised' - eSafety focus group participant, 18

[858] H Cahill et al., '*Resilience, Rights and Respectful Relationships: Teaching for Social and Emotional Learning and Respectful Relationships*', Victoria Department of Education and Training, Melbourne, 2016; UNICEF 2020.
[859] H Cahill et al., 2016.
[860] H Cahill et al., 2016; See Appendix 5.

Young people's perceptions and voice

Supporting children and young people to participate meaningfully in the design, development, and implementation of their online safety education is important – this includes education about online pornography and its impact on relationships, sexuality, respect, and consent. Youth participation and co-design can help to make sure messaging is relevant, relatable, authentic, and effective.[861]

eSafety youth engagement

In 2021, eSafety commissioned research from Professor Amanda Third and colleagues from Western Sydney University to inform eSafety's engagement strategy for young people. Participants called for more online safety education, tools and resources that directly address the key issues they face online, including access to pornography. They also called for opportunities to provide input into the establishment of processes and systems for ongoing engagement and evaluation.

In April 2022, eSafety established the eSafety Youth Council to provide young people a voice to government on online safety. The 25 Council members are aged 13 to 24 years and are from a diverse range of experiences, genders, cultural and linguistic backgrounds, and locations. The Council's role is to provide advice to government about issues young people experience online and explore ways of supporting them to have positive online experiences – including by contributing to this report.

Children and young people hold conflicting and nuanced views about online pornography. They can find it concerning, but also informative and enjoyable while still being critical of it. Education should allow for an exploration of diverse perspectives in a way that is constructive, trusting and respectful.[862] Our research found that 42% of the young people surveyed (and 58% of LGB+ young people surveyed) felt that current education about sexuality and relationships does not meet young people's needs. Only 22% said young people trust school as a source of information and advice about online pornography.

[861] A Third et al., *'Consultations with young people to inform the eSafety Commissioner's Engagement Strategy for Young People'*, Young and Resilient Research Centre, Western Sydney University, Sydney, 2021; C Wright et al., 2021; K Dawson, S Nic Gabhainn and P MacNeela, *'Toward a Model of Porn Literacy: Core Concepts, Rationales, and Approaches',* The Journal of Sex Research, 2019, 57(1):1-15; K Dawson, *'Educating Ireland: Promoting Porn Literacy Among Parents and Children'*, Porn Studies, 2019, 6(2):268-271; UNESCO 2018; A Goldstein, *'Beyond porn literacy: drawing on young people's pornography narratives to expand sex education pedagogies'*, Sex Education, 2020; K Hare, J Gahagan, L Jackson, et al., 2015.

[862] A Third et al., Western Sydney University, 2021.

> ‘It also focuses more on the biological aspect of sex and its purpose, not the more realistic things that teenagers want to/need to know’ – eSafety focus group participant, 17
>
> ‘There is too much stigma being taught, even in mandatory sex education at schools - eSafety focus group participant’, 18
>
> ‘I feel like providing more support WITHIN the school system would be more helpful than outside the system, since some kids don't have access to outside sources of information. From where I am, the sex-ed is taught horribly, and I learned more from online than my parents OR from school’ - eSafety focus group participant, 18

However, 52% believed that sexuality and relationships education had the potential to help them manage negative impacts of online pornography. The criticisms and hopes young people conveyed to us through our research is broadly consistent with other recent Australian research, which finds that programs are delivered inconsistently and received variably.[863]

Nearly three quarters (73%) of the young people we surveyed thought education and information specifically to help young people distinguish pornography from actual sex would be beneficial. [864] This aligns with consultation feedback indicating that while most young people can comprehend that pornography is not ‘real’, they have difficulty identifying which aspects are ‘unrealistic’.[865] Evidence indicates that merely labelling content as ‘unrealistic’, without further explanation, can contribute to discriminatory views about sexuality and be contrary to the experiences of young people who do in fact learn about the mechanics of sex through pornography.[866]

A strong theme in the consultations, backed up by other evidence, was that pornography can be validating and affirming for those who do not see themselves represented in mainstream media and sex education, particularly LGBTIQ+ young people.[867] Of the young people we surveyed, LGB+ young people were significantly more likely to think there were some positive effects (i.e., very positive, positive and both positive and negative) of online pornography on young people

[863] C Fisher et al., ‘*The 6th National Survey of Australian Secondary Students and Sexual Health (SSASH), The Australian Research Centre in Sex, Health and Society’*, La Trobe University, 2019; Ezer et al., 2020; TM Jones and L Hillier, *‘Sexuality education school policy for Australian GLBTIQ students’*, Sex Education, 2012, 12(4):437–454; J Power et al., ‘*The 7th National Survey of Australian Secondary Students and Sexual Health (SSASH)’*, The Australian Research Centre in Sex, Health and Society, La Trobe University, 2022.

[864] Australian students were also found to want sex education to include information about pornography in AAAH 2018: see: https://www.aaah.org.au/public/117/files/Position%20Papers%20%26%20Statements/CSE_Position_Paper_Final_31Oct2018.pdf.

[865] See Appendix 5.

[866] See Appendix 5; K Litsou et al., 2020; P Byron et al., 2021.

[867] See Appendix 5; K Litsou et al. 2020; M McCormack and L Wignall, *‘Enjoyment, exploration and education: Understanding the consumption of pornography among young men with non-exclusive sexual orientations*’, Sociology, 2017, 51(5):975-991.

learning about sex and exploring their sexuality than heterosexual young people (60% vs. 48%). Online pornography can therefore be an important source of information and expression for LGBTIQ+ young people and members of other diverse marginalised communities for whom generic sex education may not be relevant or inclusive, or who may not have access to such education.[868]

According to 2021 research from the South Australian Commissioner for Children and Young People, one third (33.5%) of LGBTQA+ students in South Australian secondary schools reported never having any aspect of LGBTQA+ people mentioned in a supportive or inclusive way during their relationship and sex health education.[869] Respondents who identified as sexually diverse were also less likely to rate their relationship and sexual health education as positive and relevant, reflecting the commonly reported disproportionate focus on male and heteronormative relationships, perspectives, and experiences.

> 'I think support should also be provided for LGBTQ relations as it's something I've never heard discussed in school and can be really dangerous for people in this community especially with the fetishisation of them in porn' - eSafety focus group participant, 17
>
> 'There is barely any education on sex in school and whatever is provided is focused on males' – eSafety focus group participant, 16

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.[870] Educators and others who play a role in the sex and relationships education of this cohort, often families, may need support to know how best to tailor education to the needs of their young people.[871]

Educators and curriculum designers may also need support to understand the value of peer-led sex education for young people with intellectual disability or who are neurodivergent.[872] Depending on the young person's experience of intellectual disability or neurodivergence, the methods, material, and frequency of sex and relationship education may differ from standard models in current curricula.[873] Importantly, educators should be equipped to deliver sex and

[868] K Hare, J Gahagan, L Jackson, et al, 2015; SSASH, 2019; A Waling et al*., 'Young people, sexual literacy, and sources of knowledge',* La Trobe University, 2019.
[869] *Sex education in South Australia: what young people need to know for sexual health and safety,* 2021.
[870] 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. (McDaniels and Flemming 2016)
[871] (Kahn and Kofke 2022).
[872] Frawley and O'Shea 2020.
[873] L Kahn and M Kofke, '*The Taboo Should Be Taught: Supporting Autistic Young Adults in Their Sexuality, Intimacy, and Relationships*', in Transitioning to Adulthood with Autism: Ethical, Legal and Social Issues, 2022, 41-61, Springer

relationships education to neurodivergent young people and young people with intellectual disability in ways that avoid ableist stereotypes. For example, the idea that autistic people are not sexual or are unlikely to form sexual relationships.[874]

When asked to identify the reasons young people may not seek help to manage the impacts of online pornography, 80% of our survey group thought feeling embarrassed about the topic and 77% felt being judged or shamed may be reasons. Young women and LBG+ young people were more likely to think it was because of feeling embarrassed (83% and 86%, respectively) or the risk of being judged or shamed (81% and 87%, respectively).

> 'Even though its more normalised I feel like there's still a bit of a stigma around it, which there shouldn't be' – eSafety focus group participant, 18
>
> 'It has a negative perception in most cultures' – eSafety focus group participant, 18
>
> 'Yeah, society usually has negative stereotypes around anything to do with porn' – eSafety focus group participant, 16

Focus group participants also said education should include information about both the potential harms and the potential positive aspects of pornography in a non-judgmental way. This echoes the findings from eSafety's youth engagement research, in which young people highlighted they want an online world and help-seeking avenues that are non-judgemental, safe and inclusive.[875] It also echoes research that suggests a core concept for pornography literacy education should be to reduce shame.[876] Young people have told us that online safety messaging should be empowering, positive, understanding, respectful, trusting, informed and constructive.[877]

> 'I think definitely for girls it should be more normalised' - eSafety focus group participant, 17
>
> 'I mean I don't think ads for porn, sharing porn and stuff like that should be normalised, I think it should be a private thing, but keep it normal to watch it for own pleasure...' - eSafety focus group participant, 16

International Publishing; Frawley, P., Wilson, N.J. *'Young People with Intellectual Disability Talking About Sexuality Education and Information',* Sex Disability **34**, 469–484 (2016). https://doi.org/10.1007/s11195-016-9460-x; McDaniels, B., Fleming, A, '*Sexuality Education and Intellectual Disability: Time to Address the Challenge,* Sex Disability 34, 215–225 (2016). https://doi.org/10.1007/s11195-016-9427-y.

[874] Kahn and Kofke 2022.

[875] A Third et al., Western Sydney University, 2021, p.34.

[876] Dawson, K., Nic Gabhainn, S. and MacNeela, P., 2019, '*Toward a Model of Porn Literacy: Core Concepts, Rationales, and Approaches',* The Journal of Sex Research, 57(1), pp.1-15.

[877] A Third et al., Western Sydney University, 2021, p19.

> ‘As long as both pros and cons are covered [in education] because then they can make an informed decision for themselves’ - eSafety focus group participant, 18
>
> ‘They should feel informed about this taboo topic and be able to make their own opinion about it’ – eSafety focus group participant, 16

Both adult experts and children and young people raised the importance of being able to ask questions. Clinical therapists we spoke to at a youth support service talked about how often children and young people wanted to know ‘am I normal?’ in relation to sex and their bodies – with pornography either giving rise to this question and/or serving as a potential source of information to find the answer.[878] A panel of Australian experts recently established a set of criteria for assessing whether pornography can support healthy sexual development for young adults.[879]

Of the young people we surveyed, 44% of the said being able to ask questions about online pornography was a way to manage its potential negative impacts. This was higher for LGB+ young people (59%) and young people with disability (57%). Our previous youth engagement research demonstrates that anonymity and confidentiality are critical factors to encouraging help seeking with these types of questions.[880]

> ‘Oh yeah. Would be great if they (children and young people) had enough healthy discussions prior to encountering porn accidentally to know if it's harmful or not’ – eSafety focus group participant, 18

Places for young people to access education

While there was some interest among stakeholders in the potential benefits of a one-stop-shop for online information,[881] there was also acknowledgement that because the issue of online pornography cuts across so many different topics, resources need to be integrated across a variety of information sources. This includes those related to body image, mental health and wellbeing, relationships, sex, sexuality, and sexual health. Depending on the relevant lens, a young person might seek information from a variety of different places, including potentially from the wellness centre of a porn site itself.[882] With mental and physical health information tailored for young people increasingly being offered online – such as ReachOut Australia and

[878] See Appendix 5.

[879] A McKee, A Dawson and M Kang, *‘The Criteria to Identify Pornography That Can Support Healthy Sexual Development for Young Adults: Results of an International Delphi Panel*’, International Journal of Sexual Health, 2023, DOI:10.1080/19317611.2022.2161030.

[880] A Third et al., Western Sydney University, 2021, p15.

[881] See Appendix 5.

[882] For example, Pornhub has introduced a Sexual Wellness Center, with content about sexual anatomy, sexual health and sexuality and relationships.

Youth Action’s Ask for Health – there is an opportunity to tap into these resources to integrate evidence-based information about online pornography.

Social media was also raised as a potential source of information (in addition to being a place where pornography was encountered, as set out in chapter 5). 35% of the young people we surveyed (43% of LGB+ young people and 41% of young women) identified social media (influencers and generally) as a trusted source of information and advice about online pornography - the highest ranked option. However, other recent research indicates social media may not be preferred.[883] Websites and support services were ranked lower among survey participants (28% and 24%, respectively), though support services rated higher among those who speak a language other than English at home (38%).

Reading about online pornography was the most preferred way to receive this information (52%), compared with watching short videos (38%) and face-to-face conversations (35%). LGB+ young people (66%) and young people with disability (61%) also expressed a greater preference for reading.

> ‘I think finding educational videos and websites to answer questions maturely and well and sharing them with the children so they can learn about it when they're ready and where they feel safe is an incredible way to go’ - eSafety focus group participant, 17
>
> ‘I think that for teenagers one of the most comfortable places is around their friends so possibly having these sorts of things on social media and stuff would make sense’ - eSafety focus group participant, 16

[883] C Wright et al., 2021.

Educating children and young people about online pornography

While it is largely accepted that age-appropriate education about the broad concepts of consent, respect and online safety should start from the earliest ages, stakeholders consulted for the roadmap offered differing perspectives about the age at which pornography-specific education should be introduced.

Some stakeholders suggested that late primary school (ages 8 to 10) is a suitable time to start having conversations with children about this topic in a developmentally appropriate manner, using less explicit language than may be used for older cohorts.[884] As set out in chapter 5, 39% of the young people eSafety surveyed first saw online pornography before they were 13, and there is anecdotal evidence from educators indicating that some children are accessing online pornography as early as Years 1-2.

However, there is a level of discomfort and uncertainty around whether, and how, to have discussions with children in this age group in a way that promotes their best interests.[885] For example, Trusted eSafety Providers have advised that some primary schools are hesitant to permit discussions of online pornography in broader online safety lessons due to concerns about appropriateness and student wellbeing. This reticence is not limited to adults – young people in our focus groups also felt there was some discomfort associated with learning about these subjects in school.

> ‘I think it's a topic that some people just find uncomfortable in general’ – eSafety focus group participant, 18

Some stakeholders recommended that pornography literacy education should start from approximately 11 years old,[886] while others suggested initiating education about pornography in years 9 to 10, as this is where the subject matter connects most strongly to curriculum (i.e., sexuality, consent and respectful relationships). [887] Notably, international guidance developed by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) suggests that discussions of online pornography literacy and gender stereotypes should begin from ages 9-12.[888]

[884] See Appendix 5.
[885] K Albury, ‘*Young people, media and sexual learning: rethinking representation*’, Sex Education, 2013, 13(1): S32-S44, DOI: 10.1080/14681811.2013.767194
[886] See Appendix 5.
[887] See Appendix 5.
[888] UNESCO, 2018.

The divergence in views was not limited to adult stakeholders. Some young people in our focus groups felt that education about online pornography should be available earlier given that some children are seeing the material at young ages, others felt that a higher level of maturity and understanding would be important for education to be effective. However, stakeholders agreed that programs and resources should be underpinned by established good practices in online safety, sexuality, respectful relationships and pornography education.

> ‘Better education at a younger age, things like sex ed aren't getting taught at schools until around grade 5 or 6, most kids have access to the internet well before that, and can be exposed to these things before they have been educated on it’ – eSafety focus group participant, 17
>
> ‘I think it depends on the age, like most schools do it early on in younger years but I think the lack of maturity and understanding takes away from what is being taught’ - eSafety focus group participant, 17
>
> ‘It's hard to find the age where it's not too early because you don't want to make young kids aware of it to be curious, but then you don't want them to come across it uneducated’ - eSafety focus group participant, 16

Current school-based education

Education authorities and providers we consulted shared incidents at school involving students’ use of pornography. These stakeholders have observed an increase in reports from teachers and students of peer-to-peer sharing of online pornography in school environments and noted this was happening in primary schools as early as year 1 or 2. Some perceived a normalised culture of pornography by the time students reach secondary school, with some students reportedly watching online pornography while at school. There was particular concern that the type of content being viewed tends to display sexism and violence toward women, and that this is contributing to boys sexualising, harassing or assaulting girls at school (for example, groping or up-skirting).

In addition to these overt forms of harassment and abuse, the viewing of pornography on schoolgrounds can contribute to a hostile, humiliating or intimidating school culture. While this may be most pronounced in co-educational environments, education providers also observed a growing demand for education sessions about online pornography in boys’ schools. Students may feel pressure to support this type of culture, and any negative attitudes and behaviours towards girls and women they develop within this context can inform their broader interactions outside school settings.

Consistent with the good practice frameworks outlined below, we heard in our consultations that achieving an inclusive, shame-free and effective educational response to online pornography within the school setting requires a whole-school approach. This 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.

Stakeholders have emphasised the importance of integrating online pornography education into the curriculum.[889] Consultation participants pointed out that schools across Australia may be at different stages in transitioning from a biology-focused approach to sex education to a more contemporary approach. They noted there are opportunities to enhance the F-10 Health and Physical Education curriculum, including sexuality and health, respectful relationships and consent, media and digital literacy, and digital citizenship and online safety. Participants also highlighted that age and stage-appropriate lessons should be delivered consistently across each schooling year.

While several jurisdictions 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. Some education sectors and individual schools provide a variety of teaching and learning activities through designated curriculum, wellbeing time and/or external providers.

The Australian Curriculum

The recently updated Australian Curriculum (version 9), developed by ACARA following the 2020-21 Australian Curriculum Review, embeds online safety for Foundation to Year 10 across learning areas and the general capabilities.

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

[889] See Appendix 5.

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.

- **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.

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.

Addressing online pornography in online safety education

Pornography education has been endorsed in recent national prevention frameworks and plans of action and is increasingly delivered in Australian schools as a component of respectful relationships curricula.[890]

In 2019, eSafety commissioned Professor Kerryann Walsh and colleagues from the Queensland University of Technology to undertake research into existing best practice in online safety education.[891] This research provided a foundation for eSafety's Best Practice Framework for Online Safety Education[892] which establishes a nationally consistent approach for delivering high quality online safety education programs in Australia and implementing a whole-school approach to creating a safe online environment.

The research identified that the risk of children encountering pornography should be addressed within online safety education.[893] Specifically, it suggested relevant education should:

- include sex education which can help counter negative effects of viewing pornography
- address the messages that boys take from pornography and their expectations for the girls with whom they interact
- address the messages that girls take from pornography and how they may be influenced within actual or potential sexual relationships
- consider gender equality — drivers of gender-based violence (overlap with sexual violence, above)
- explore what sexual harassment is
- look at coercion and consent in relationships
- include victim blaming and shaming
- include sharing of self-generated sexual images and videos (aggravated/deliberate/experimental).

[890] ACARA, *Australian Curriculum: Respect matters | The Australian Curriculum (Version 8.4)*, n.d., https://www.australiancurriculum.edu.au/resources/curriculum-connections/portfolios/respect-matters/

[891] eSafety Commissioner, *'Best Practice Framework for Online Safety Education (Stage 1)',* eSafety website, 2020, available at: https://www.esafety.gov.au/educators/best-practice-framework.

[892] eSafety, *Best Practice Framework for Online Safety Education (Stage 1).*

[893] See Table 9: Violence Prevention in eSafety, Best Practice Framework for Online Safety Education (Stage 1).

Strengthening sexuality and respectful relationships education

UNESCO has produced international technical guidance on sexuality education which includes many elements of eSafety's Best Practice Framework.[894] The guidance highlights that sexuality education should be scientifically accurate, incremental, age- and developmentally appropriate, curriculum-based, comprehensive, culturally relevant and based on human rights and gender equality. It also emphasises the importance of evaluation, and that sexuality education should support children and young people to develop the life skills they need to make informed and healthy choices. The guidance recognises that schools play a central role, but non-formal and community-based education is also important.

The guidance suggests that discussions of pornography, how it portrays men and women, and how to talk to a trusted adult about it should be incorporated in sexuality education from age 9-12 and expanded on in subsequent lessons for 12-15- and 15–18-year-old age groups.

As explored in chapter 5, aggressive and seemingly violent acts are common in mainstream online pornography. While not all 'rough' sex depicted in pornography is non-consensual, it is rare for discussions on consent to be included.[895] Children – especially younger children – may have difficulty understanding how these depictions relate to real-life intimacy. Overall, the 16–18-year-olds we surveyed displayed a capacity to critically engage with pornography, and a majority thought the effect of online pornography on young people's expectations about sex, ideas about intimate relationships, understanding of consent and views about gender is negative.

Research and our consultations pointed to the importance of providing balanced and non-judgemental education and support for children and young people to navigate these issues. Stakeholders advised that children and young people need to be able to ask questions both proactively and in response to any concerns they may have developed about their use of online pornography or harmful behaviour they have either engaged in or experienced which relates to pornography.

[894] UNESCO 2018.

[895] M Willis et al., *'Sexual Consent Communication in Best-Selling Pornography Films: A Content Analysis'*, The Journal of Sex Research, 2020, 57(1):52-63, DOI: 10.1080/00224499.2019.1655522.

Proposed school-based framework for addressing pornography's influence on young people

Broadly aligned with both frameworks, Maree Crabbe and Michael Flood have developed proposed practice framework for school-based education that addresses pornography's influence on young people.[896] Many of the good practice concepts were echoed in other research submitted to, or conducted by eSafety, as well as through the consultations.

The Crabbe and Flood framework consists of 14 elements:

1. A whole-school approach, coordinated across the domains of:
   - curriculum, teaching and learning
   - formal school policies and practices
   - school culture, ethos and environment and
   - the relationships between school, home and community.
2. A robust conceptual approach, which includes:
   - **a**n evidence-based understanding of pornography's prevalence, nature and impact on young people
   - a critical understanding of gender, power and violence
   - a positive approach to sexuality
   - an understanding of and responsiveness to diversity
   - a human rights orientation
   - a harm minimisation and strengths-based approach.
3. A tailored approach to make sure it is appropriate, relevant and inclusive – while maintaining the integrity of a robust conceptual framework.
4. Based in sexuality education as the most relevant curriculum context, while also supported and extended in other areas such as humanities, social sciences, technology and the arts.
5. Builds student competencies, including:

[896] M Crabbe and M Flood, 2021.

  - analysing social, cultural and societal influences that shape identity and affect wellbeing
  - understanding the characteristics of healthy and unhealthy relating
  - communicating and interacting for wellbeing.

6. Age-appropriate and sequential delivery emphasising three different learning strategies – foundational, integrated and specific – as it moves from younger to older cohorts of children.
7. Participatory teaching and learning approaches, which model respectful, inclusive relationships while encouraging critical thinking and personalised learning.
8. A safe, inclusive, supportive learning environment, which is mindful of gender, age, cultural background, religion, sexual orientation, maturity level, exposure to pornography, and experiences of violence.
9. Sensitivity to inequalities of gender, sexuality and race/ethnicity and the ways stereotypes and power dynamics can manifest in pornography.
10. Skilled, well-equipped staff with competencies across sexuality, gender and violence prevention.
11. Active engagement of parents as partners, employing strategies to manage potential resistance, including by equipping parents with appropriate knowledge, skills and resources.
12. Development of community partnerships which can provide expert support and facilitate referral of students to specialist services where needed.
13. Support across the school organisation, culture and environment, including its leadership, policy and practices.
14. Regular evaluation and review to ensure the approach is effective, relevant, appropriate and responsive to emerging needs and technologies.

Consistent with the good practice frameworks highlighted above, 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,[897] as young people often turn to their peers for support and advice about sex and relationships. When asked who young people trust for

[897] eSafety Commissioner, *Thematic analysis of age verification submissions*, eSafety website, n.d., available at: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification#thematic-analysis-of-age-verification-submissions:~:text=to%20online%20pornography.-,Thematic%20analysis%20of%20age%20verification%C2%A0submissions,-This%20summary%20is; See Appendix 5.

information and advice about online pornography, one third of our survey participants selected peers with similar experiences. The preference for peer support was higher among LGB+ young people (40%). Experts noted that young people often have the capacity and resilience to navigate complicated issues among themselves, with the right information and support.[898]

Sexual Health Victoria – 'Youth Cybersafety, Relationships and Sexuality'

With the support of eSafety's Online Safety Grants Program, Sexual Health Victoria (SHV) is developing and piloting a whole-school education program designed to bridge the gap between early adolescents' understanding of online safety and the connection to healthy relationships and sexuality. It is aimed at:

- parents and carers of young people aged 10-14 years
- school teachers, school leaders and wellbeing teams
- young people aged 10-14 years.

The program has been co-designed in consultation with schools, young people and families and is currently being piloted in government and independent primary schools (Years 5-6) and secondary schools (Years 7-8) in Melbourne and regional Victoria. The program consists of:

- professional learning and resources to build teacher skills and confidence
- instruction on how to facilitate the education sessions
- a series of webinars
- a seven-part podcast series
- an eLearning module to support discussion of online sexual content and behaviours age appropriate in-class education sessions for young people.

'should be a safe environment, where the message doesn't make porn look like a bad thing, but should definitely highlight the cons' – eSafety focus group participant, 18

'If you understand the negative effects, then you can mitigate them and make online pornography a positive experience' – eSafety focus group participant, 17

'I think that learning how to distinguish porn from reality would be a good start - eSafety focus group participant', 18

[898] See Appendix 5.

Education as violence prevention

Our Watch is a national leader in the primary prevention of violence against women and children in Australia. Its 2020 background paper, Pornography, young people and preventing violence against women, explores the relationship between young people's access to pornography and the development of the kinds of attitudes and beliefs that are known to drive violence against women. The paper finds that pornography both contributes to and reinforces the kinds of social norms and attitudes that have been identified as drivers of violence against women. There is a strong rationale for the development of holistic primary prevention initiatives that work with children and young people and the community around them, and across policies, programs and education materials to address the influence of pornography.

Consistent with the themes explored in this chapter, Our Watch's key recommendations for work in this area include:

- producing tools and resources for parents, carers and guardians
- producing information and practical tools and resources specifically for young people
- including the topic of pornography in respectful relationships education
- professional education and development for teachers on the topic of pornography resources and training for other professionals who work with young people.

Our Watch- Respectful Relationships Education Toolkit

An evidence-based approach to comprehensive respectful relationships education in schools. This Toolkit provides support and advice regarding a whole-school approach in addition to curriculum links and best-practice regarding respectful relationships. It includes the evidence, background information and components of a whole-of-school approach to preventing gender-based violence in schools. It outlines the actions to undertake when implementing a whole-school approach. The resource acknowledges that each school is 'unique and will be at different stages of addressing gender-based violence and promoting respectful relationships, non-violence and gender equality.'

In 2021, the Department of Education contracted the Monash Gender and Family Violence Prevention Centre to undertake a national stocktake and gap analysis of respectful relationships education material and resources.[899] The stocktake identified the need for greater coordination across government at the Commonwealth, State and Territory levels, and recommended the creation of a national coordination mechanism for respectful relationships education and policy.

The stocktake identified several programs which include content about online pornography:

- The Commonwealth funded *The Practical Guide to Love, Sex and Relationships*[900] developed by the Australian Research Centre in Sex, Health and Society at La Trobe University. This sexuality education resource for students in years 7-10 has used Moira Carmody's sexual ethics decision framework and includes the topic of pornography.
- Maree Crabbe's *It's Time We Talked*[901] has a specific focus on pornography and takes a whole school approach. It was developed from research with young people in the community and includes teacher and school professional development as well as teaching and learning activities.
- SHINE SA's *Teach it like it is*[902] utilises strengths- and Inquiry-based learning to enable students to develop health literacy skills and explore ethics and community attitudes to issues of sexuality and relationships, including activities examining pornography. The resource can only be obtained if teachers undertake the Relationships and Sexual Health Curriculum professional development program.

[899] N Pfitzner et al., '*Respectful Relationships Education in Australia: National Stocktake and Gap Analysis of Respectful Relationships Education Material and Resources Final Report*', Monash University, 2022, DOI:10.26180/21099592.v1.

[900] The Australian Research Centre in Sex, Health and Society, '*The Practical Guide to Love, Sex and Relationships*', La Trobe University, 2015, available at: https://www.lovesexrelationships.edu.au/

[901] Maree Crabbe, '*It's time we talked*', available at: https://itstimewetalked.com/

[902] Shine SA, '*Teach it like it is*', available at: https://shinesa.org.au/activity/primary-years/

Reducing stigma and improving inclusivity

Experts engaged in our consultations pointed out that some research and educational programs about the harms associated with children's access to pornography may be based on biased notions of harm. For example, where specific sex acts or practices are categorised as inherently harmful based on heteronormative, ableist and/or kink phobic assumptions.[903] Sex workers also highlighted that narratives around pornography and harms to children often cast them as predators or perpetrators rather than as important stakeholders and potential collaborators in developing education.[904] They may have an especially important role to play in education tailored for LGB+ young people, who indicated they were more likely than heterosexual young people to seek information and advice about online pornography from people working in the adult industry.

Some participants in our focus groups also associated online pornography with stigma and shame, and research submitted to our call for evidence indicates that the discourses around the harms of pornography have the potential to exacerbate anxiety and shame for young people.[905] Many focus groups participants called for de-stigmatisation of viewing pornography to provide more constructive and safe spaces for discussing risks and harms. Consultation participants also called for de-stigmatisation of sex work, and greater respect for the rights of performers.[906]

It is important to note that it is not only the narratives *about* pornography that reflect bias, but also the narratives perpetuated *within* pornography which can be deeply problematic. There is evidence that mainstream pornography often uses overtly racist language and reflects discriminatory views and tropes about same sex attracted people, women, gender roles, and racial or ethnic stereotypes.[907] Education about online pornography should be sensitive to these issues and how they may affect students.

[903] See Appendix 5; P Byron et al., 2021; A McKee*, 'Methodological Issues in Defining Aggression for Content Analyses of Sexually Explicit Material'*, Archives of Sexual Behaviour, 2015; A McKee et al., '*The relationship between consumption of pornography and consensual sexual practice: Results of a mixed method systematic review*', The Canadian Journal of Human Sexuality, 2021, 30(3):387-396; K Wilson, D Wiley and B Rosen, '*Texas Sexuality Education Instruction: Shame and Fear-Based Methodology*', Journal of Health Education Teaching, 2012, 3(1);1-10.

[904] See Appendix 5.

[905] 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'*, Sex Education, 2016, 16(2):130-142.

[906] See Appendix 5.

[907] M Crabbe and M Flood, 2021; W DeKeseredy and A Hall-Sanchez, *'Adult pornography and violence against women in the heartland: Results from a rural southeast Ohio study',* Violence Against Women, 2017, 23(7):830–849. DOI: 10.1177/1077801216648795; G Dines and C West, '*White Girl Moans Black Lives Matter*' Pornhub's #BLM genre and the industry's brash racism, Slate website, 2020; Y Mirzaei, S Zare and T Morrison*, 'Hijab Pornography: A Content Analysis of Internet Pornographic Videos*', Violence Against Women, 2022, 28(6–7):1420–1440, DOI:10.1177/10778012211021125; M Donevan, *'If pornography is sex education, what does it teach?'*, in M Kiraly M and M Tyler M (eds) Freedom Fallacy: The Limits of Liberal Feminism, Connor Court Publishing, Ballarat, Australia, 2015.

Some young people in eSafety's focus groups emphasised that education should be sex-positive and non-judgmental. They suggested that ideally, education on these subjects should feel open, friendly, comfortable, safe, neutral, calm, funny and casual.

> 'I think we should be able to create a safe space to discuss/learn/educate. So, like while people can enjoy it at least they can be aware that it's not the most realistic thing, and not just for relationships but also for body image, consent, and how sex works etc' – eSafety focus group participant, 18
>
> 'I think it should be taught in a way that doesn't make porn seem evil and life ruining, but in a way where kids know how to be safe, and to know that it isn't what real relationships are like' – eSafety focus group participant, 17
>
> 'It should be relatable and include real life examples so a young person can understand this type of stuff is ok in real life' - eSafety focus group participant, 16

Resources which aim to reduce stigma and build inclusivity

Burnet Institute – 'The Gist'[908]

The Gist is a digital education program designed to reduce the harms of pornography for young people and prepare them for the future with alternative information about sex and relationships.

The Gist prototype was co-designed with at-risk young people aged 14-21 and was informed by best practice sexual health education and a sexual ethics framework. It provides young people with alternative, healthy and inclusive representations of sex and relationships that aim to disrupt problematic messages they may see in some pornography.

Online Safety Grants Program funding is being used to turn prototype into multi-modal education programs which aims to support sexual health and wellbeing and positively impact attitudes related to violence against women.

It is being delivered as an integrated intervention package, in a series of 10 weekly workshops with participants in up to 10 youth services in regional and metropolitan Victoria. It will also be supported by the creation of a mobile app.

The Line[909]

The Line is Our Watch's flagship digital campaign for young people aged 14 and over. Its digital content and tools for young people include hundreds of online articles, quizzes, clips and

[908] Burnet Institute, *The Gist*, available at: https://www.burnet.edu.au/research/projects/the-gist/.
[909] Our Watch, *The Line: Sex, Dating and Relationships*, available at: https://www.theline.org.au/.

interviews on having healthy and equal relationships. It talks about what is okay and what is not okay when it comes to sex, dating and relationships, and includes content about critically analysing online pornography. The campaign also includes resources and materials for parents and carers, educators and prevention practitioners working with young people, to support the holistic adoption of positive gender norms.

Kids Helpline[910]

Kids Helpline is a free and confidential 24/7 online and phone counselling service for children and young people aged 5 to 25. The website provides age-segmented advice on a range of issues for children aged 5-12, teens aged 13-17 and young adults aged 18-25. According to the Kids Helpline 2021 annual report, its web page on the impacts of pornography was the third top issue accessed on its site by young adults aged 18-25 in 2021 (4,021 views).[911]

New Zealand Porn Week[912]

In November 2022, New Zealand non-profit online safety organisation, Netsafe, held a nationwide ‘Porn Week’. The campaign, supported by an interactive website, aimed to raise awareness about sex, pornography, image sharing and consent and encourage young people to have a mature, open conversation about these topics. It provided tips for young people built around the following questions:

- Is watching porn okay?
- Can porn affect me?
- If porn’s just a fantasy, what’s wrong with watching it?
- How do you know if you’re addicted to porn?
- I feel confused about my own reaction to porn
- Is ethical porn okay?
- How do I cut back on porn?
- How do I watch porn in a healthy way?

[910] Yourtown, *Impacts of Pornography*, available at: https://kidshelpline.com.au/young-adults/issues/impacts-pornography.
[911] Yourtown, ‘*Kids Helpline 2021 Insights report*’, Yourtown website, 2022, available at: https://www.yourtown.com.au/sites/default/files/document/Kids-Helpline-Insights-Report-2021.pdf.
[912] NetSafe NZ, *‘Porn week*’, available at: https://netsafe.org.nz/porn-week/.

Keep It Real Online[913]

Keep It Real Online is a New Zealand Government public awareness campaign led by the Department of Internal Affairs.

One element of the campaign is The Eggplant, a drama/comedy online web series launched in December 2020 to help young Kiwis aged 12-18 navigate a series of issues, including using pornography to learn about sex. About 88% of parents and carers surveyed, whose children had watched The Eggplant, said it prompted a conversation about online or digital safety.

The campaign also included a series of advertisements showing parents and carers how to help their children and young people manage online issues, including access to pornography. The pornography-focused advertisement features actors portraying adult performers in a way that engages them as equal partners in educating children and young people, and a parent who tells her son she wants to talk to him with 'no judgment'.

Porn is not the norm[914]

Porn Is Not the Norm is a new initiative being delivered by Interchange Outer East. It aims to prevent autistic young people from being harmed by pornography through equipping them and their parents, carers, teachers and workers to understand pornography's prevalence and potential impacts, and how they can safely navigate healthy and respectful relationships and sexuality in this context. It will include education events and resources for autistic young people, parents and carers, as well as professional learning for teachers and others.

[913] New Zealand Department of Internal Affairs, '*Keep it real online'*, available at: https://www.keepitrealonline.govt.nz/about-us/.
[914] Porn is not the norm, '*Young people, autism and the impact of porn*', Not the norm website, n.d., https://notthenorm.com.au/

Empowering parents to educate their children about online pornography

eSafety's 2018 research with Australian parents of children aged 6-17[915] shows that access to pornography was one of their top five concerns, with 33% of respondents identifying it as a main risk of their children's internet use. For those parents who became aware their child had encountered online pornography, 61% reported their response was to speak frankly to their child about it. While most parents (69%) expressed confidence in their ability to deal with their children encountering online pornography, a quarter (25%) said they would be embarrassed to talk to their children about pornography.

Submissions and consultations also highlighted the need for education and information about how to access and apply safety technology and tools, such as parental controls and search filters. [916] These technologies can help parents and carers to protect children from a range of online risks and harms beyond access to pornography, including grooming and other forms of abuse. Online services and industry associations highlighted a variety of resources provided by social media services, search engines, internet service providers, telecommunications companies and others to support parents in this regard.[917] Some also 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.[918] Stakeholders noted this was an area where government could assist, including potentially through the creation of an online hub for parents to access information and online safety tools or programs.[919]

Family Friendly Filters

The Communications Alliance leads the Family Friendly Filter program[920]. This program promotes filtering products to consumers which have been accredited through independent testing for effectiveness, ease of use, configurability and availability of support. More information on Family Friendly Filters can be found in chapter 11.

[915] eSafety Commissioner, *Parenting and pornography summary report, https://www.esafety.gov.au/sites/default/files/2019-09/summary-report-parenting-and-pornography.pdf*.
[916] eSafety, *Summary of Call for Evidence on Age Verification*; See Appendix 5.
[917] See Appendix 5.
[918] See Appendix 5.
[919] See Appendix 5.
[920] Communications Alliance, '*Family Friendly Filter Program*', available at: https://www.commsalliance.com.au/Activities/ispi/fff.

The Communications Alliance also points to information about online safety and parental controls provided by Internet Service Providers, including Aussie Broadband [921], FOXTEL[922], iiNet[923], Optus[924], Telstra,[925] TPG[926] and Vodafone.[927]

Parental and caregiver involvement in the online lives of children and young people plays an important role in promoting safe online experiences. Research demonstrates that where children's encounters with pornography result in harm, that harm often stems from the subsequent negative reactions of trusted adults (such as anger or shame) as opposed to the material itself.[928] This may be especially so in 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. Roadmap consultations also highlighted that parents who are less familiar with these issues, and less comfortable using technology, can be more restrictive of their children's internet use due to fears of online harms, including access to pornography. They noted this can result in children and young people missing out on beneficial educational content and social interactions and emphasised the importance of a balanced approach.[929]

A third of the young people we surveyed said parents are not equipped to support young people in relation to online pornography (41% of LGB+ young people) and 38% said education should be provided to parents and carers so they can better support young people with this issue. This echoes the findings from our youth engagement research, in which participants called for targeted resources for parents and other trusted adults so they can provide information and support without judgment.[930]

> 'Well at home (learning about sex and/or pornography) might be uncomfortable since some people's parents have religious backgrounds which are very against the idea of porn' – eSafety focus group participant, 17

[921] Aussie Broadband, *'How to educate your children about cyber safety'*, available at: https://www.aussiebroadband.com.au/blog/how-to-educate-your-children-about-cyber-safety/

[922] Foxtel, *'Parental controls'*, available at: https://www.foxtel.com.au/support/broadband/wifi-modem/parental-controls.html.

[923] iiNet, *'Filtering*', available at: https://www.iinet.net.au/about/legal/filtering/.

[924] Optus, *'Internet security*', available at: http://www.optus.com.au/internetsecurity.

[925] Telstra, *'Cyber security and safety*', available at: https://www.telstra.com.au/cyber-security-and-safety.

[926] TPG, '*Online safety'*, available at: https://www.tpg.com.au/about/online_safety.php.

[927] Vodafone, *'Digital parenting*', available at: http://www.vodafone.com.au/about/sustainability/digital-parenting.

[928] See Appendix 5; D Buckingham and S Bragg, *'Opting in to (and out of) childhood: young people, sex and the media'*, in J Qvortrup (eds) Studies in Modern Childhood: Society, Agency, Culture, Houndsmills, Palgrave Macmillan, Basingstoke, 2005, 59-77; S Spišák, 2016.

[929] See Appendix 5; eSafety's Mind the Gap research similarly found that children with restrictive parents are less likely to be engaging in supportive and protective online activities.

[930] A Third et al., Western Sydney University, 2021.

> ‘Some responsibility should be schools and others should be parents. Sometimes it's hard for parents to educate though because some aren't as tech-savvy as others’ - eSafety focus group participant, 16
>
> ‘Also, while education [is important for] the children, the parents should undergo a similar program, so that they are working hand in hand and its more holistic education, as that way it's not up to the child to continue the conversation at home’ – eSafety focus group participant, 18

"As at June 2018, 41% of parents reported having had a conversation about pornography with their children. This increased to 67% of parents of children aged 13–17. Of the parents yet to talk to their children, 39% thought the best time was between the ages of 10–12. Just over a quarter (27%) of parents would instead wait until their child was a teenager or older, while 9% felt the best time to talk to their child was 9 years or younger.

About 22% felt it was best to wait until the issue came up. However, in our consultations, experts expressed that waiting for children to start the conversation can be too late as it suggests they may have already encountered pornography.[931] As outlined above, good practice is to start introducing foundational online safety concepts to children from the youngest ages and build on these discussions over time. By engaging in regular conversations about online safety, parents and carers can support children and young people to be safe, and feel safe, and help them build the skills to manage risks and benefits from the opportunities to learn and engage online. According to eSafety’s 2021 *Mind the Gap* research, only about half of the parents whose 14–17-year-old children had seen sexual images on the internet or opened a message or link showing pictures of naked people, were aware their children had seen this material.

eSafety Parent Resources

eSafety provides a range of advice and resources to support parents and carers to start the chat, including ‘Online porn’[932] and ‘Hard to have conversations’[933]. This advice is segmented by developmental stage, including advice targeted to parents and carers of young people aged 5-12 and 13-17. This content is currently under review, and the findings from this report will feed into that process. Support for parents and carers is also available from online safety education providers who have been endorsed under the Trusted eSafety Provider Program[934]. eSafety provides various advice for parents and

[931] See Appendix 5.
[932] eSafety Commissioner, *‘Online porn*’, available at: https://www.esafety.gov.au/parents/issues-and-advice/online-porn.
[933] eSafety Commissioner, *‘Hard to have conversations*’, available at: https://www.esafety.gov.au/parents/issues-and-advice/hard-to-have-conversations.
[934] eSafety Commissioner, *Trusted eSafety Provider Program*.

carers on how to choose and use parental controls[935], including video content[936], factsheets including parental controls in social media[937], games and apps[938],

and parental controls on devices and accounts[939].

France's 'I protect my child'

The French Government, in partnership with parenting support groups, child protection associations, and online services, recently launched I protect my child [940], a digital parenting information and support platform. It includes a dedicated section about children's access to online pornography[941], with a quiz that enables parents to find suitable safety tech tools for their family based on their children's age(s) and the device(s), operating system(s), fixed or mobile internet service provider(s) and sites or apps they use.

Raisingchildren.net.au[942]

This Australian parenting site has information on its website about how to talk to children aged 12-18 about pornography.

It is important to equip parents and carers with the right information and tools to have sufficient information to confidently address these issues. This includes information about how to prevent their child or young person from accessing online pornography, as well as information about how to talk to them about pornography in a helpful, supportive, and shame-free way to prevent and mitigate harm if, and when, they do encounter it. 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. It should also consider parents' preferred sources of information.

According to our 2018 research, when looking for advice, a parent's most common source was family and friends (36%), followed by the internet (33%) and their child's school (24%). Parents

[935] eSafety Commissioner, *'Parental controls*', available at: https://www.esafety.gov.au/parents/issues-and-advice/parental-controls.
[936] eSafety Commissioner, '*Parental controls'*, available at: https://vimeo.com/612389757.
[937] eSafety Commissioner, *'Parental controls: social media*', available at: https://www.esafety.gov.au/sites/default/files/2021-04/Parental controls in social media%2C games%2C and apps.pdf.
[938] eSafety Commissioner, *'Parental controls: games and apps*', available at: https://www.esafety.gov.au/sites/default/files/2021-04/Parental controls in social media%2C games%2C and apps.pdf.
[939] eSafety Commissioner, '*Parental controls: devices and accounts'*, available at: https://www.esafety.gov.au/sites/default/files/2021-04/Parental controls on devices and accounts.pdf.
[940] French Republic, *'I protect my child (translated)'*, \French Government website, n.d., available at: https://jeprotegemonenfant.gouv.fr/pornographie/.
[941] French Republic, *'I protect my child (translated)'*.
[942] Raisingchildren.net.au, *'Pornography – talking with teens*', available at: https://raisingchildren.net.au/teens/entertainment-technology/pornography-sexting/pornography-talking-with-teens.

and carers should also be offered digital literacy education and training so they can support their child to engage with, and navigate, digital technologies safely.

Addressing the needs of people from culturally and linguistically diverse backgrounds

We know some families, such as those from culturally and linguistically diverse backgrounds, can face additional challenges accessing online safety information and having conversations with their children about online harms. In addition, the young people eSafety 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.

Recent research commissioned by eSafety showed that culturally and linguistically diverse parents and carers worry that adopting a hard-line approach or trying to stop their children from engaging in risky or culturally unacceptable behaviours will push them further away.[943] Several participants identified that refusing to talk to their children about taboo subjects such as sex may cause them to seek information from elsewhere, which could potentially be both shameful (if others in their community find out) or dangerous, depending on where or who they sought information from.

As part of its Families Capacity Building Project, eSafety is developing online safety resources to better support a range of vulnerable communities. Online Safety for Every Family is a new package of resources that aims to help parents and carers from all backgrounds better understand online risks and work through challenges that may arise. [944] The resources are available in Plain English, Simplified Chinese, Arabic, Vietnamese, Tamil and Dari.

[943] eSafety research, unpublished.
[944] eSafety Commissioner, *'Online Safety for Every Family'*, eSafety website, n.d., available at: https://www.esafety.gov.au/parents/resources/online-safety-for-every-family.

Support for those working with children

Educators

Like parents and carers – and in line with good practice frameworks – educators must 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 so the school and its staff are prepared to address any pornography-related incidents that arise either at school or within the school community.

Consultation participants within the education sector reported that the level of confidence in discussing these issues with students varies widely. While some teachers and school wellbeing staff are highly trained and well equipped for these discussions, many others feel inadequately prepared and resourced to discuss pornography with students. They may know very little about the nature of contemporary online pornography or the digital media cultures in which it is shared, feel uncertain about whether a student's questions indicate they are at risk of harm or require action under the school's child safety policies, or they may have their own lived experiences which make the subject difficult for them.[945] In addition, they need tailored material that allows them to have safe and age-appropriate discussions based on whether they teach in early education, primary or secondary school.

Professional learning and guidance can be provided to educators in various ways and at different times, including 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 than into pre-service training curriculum, as there may be more opportunities to update it to reflect developments over time.[946] They also felt the content should help educators not only to speak to students, but also to speak to parents and carers, who may themselves be unprepared or uncomfortable to have these discussions.[947] In addition, to achieve a whole-school approach, training must be bolstered through complementary policies and procedures and a supportive and inclusive school culture.

[945] See Appendix 5; K Albury, *'Porn and participation: implications for learning and teaching practice'*, Porn Studies, 2018.
[946] See Appendix 5.
[947] See Appendix 5.

eSafety resources[948]

eSafety has developed accredited teacher professional learning for F-12 educators, wellbeing and school leaders, all of which incorporate a respectful relationships approach. The material covers online harmful sexual behaviour, misinformation, and emerging technologies.

Victorian Department of Education and Training[949]

The Resilience, Rights and Respectful Relationships learning materials have been designed for teachers in primary and secondary schools to develop students' social, emotional and positive relationship skills. This includes Building Respectful Relationships: Stepping Out against Gender-Based Violence, a set of sequential teaching activities designed for students in Years 8, 9 and 10. Elements focus on developing students' understanding of the link between sexualisation, pornography, gender-based violence, power, and respectful relationships.

Family Planning Australia

Offers professional learning for educators, Let's Talk: Technology, Sex and Relationships[950] and All About Sex resource sheets[951] for those with an intellectual disability. Technology, Sex and Relationships training for K-10 Personal Development, Health and Physical Education teachers includes details regarding pornography – as do the resource sheets available.

Teacher training in New Zealand[952]

In New Zealand, the Classification Office and the Ministry of Education teamed up to create a module for teachers on 'changing the conversations around pornography'. This open access, web-based training aims to equip teachers to support young people to critically examine the influence of pornography on their personal identity, relationships with others and the wider wellbeing of people in society.

[948] eSafety Commissioner, *'Teacher professional learning*', available at: https://www.esafety.gov.au/educators/training-for-professionals/teachers-professional-learning-program.

[949] Victorian Department of Education, Resilience, Rights and Respectful Relationships learning materials, available at: https://fuse.education.vic.gov.au/ResourcePackage/ByPin?pin=2JZX4R.

[950] Family Planning Australia, '*Let's Talk: Technology, Sex and Relationships*', available at: https://www.fpnsw.org.au/technology-sex-and-relationships.

[951] Family Planning Australia, *'All about sex*', available at: https://www.fpnsw.org.au/factsheets/individuals/disability/all-about-sex.

[952] New Zealand Ministry of Education and New Zealand Classification Office, *'Changing the conversations about pornography*', available at: training.education.govt.nz/pages/mediacontent.jsf?mediaId=1251799&catalogId=849811&menuId=112475&client=external.

Frontline workers

Families and schools are a significant source of information and support. However, some children – especially those lacking steady home environments and consistent school engagement – may not have a clear path to such support or a responsible trusted adult in their lives to discuss their questions and concerns regarding sexuality and pornography. 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.

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.[953] As specialists in this field, they noted they are uniquely well equipped to have these conversations and suggested workers in other fields could benefit from training and support.

Submissions to our call for evidence suggested that training and resources should be provided to frontline workers in health, youth, flexible learning, justice and community services to equip them to discuss online pornography with children in an informed, safe and judgement-free way.[954] Consultation participants felt that residential care, youth and allied health workers in particular should be upskilled on a broad range of online safety issues – including access to pornography – as well as the signs that a child may be having negative online experiences and how to respond.[955] Some suggested that healthcare providers should be trained to speak with patients about online pornography and safe sex practices, noting that law enforcement data indicates increasing numbers of teenage girls presenting for medical treatment for injuries sustained through sexual activity that may be influenced by online pornography.[956]

eSafety Frontline Worker Training

Within eSafety Women's Frontline Worker Technology-Facilitated Abuse (TFA) Capacity-Building Programs, online pornography is integrated as a part of the resources and professional development program to upskill frontline workers who support women

[953] See Appendix 5.
[954] eSafety Commissioner, *Summary of Call for Evidence on Age Verification*.
[955] See Appendix 5.
[956] See Appendix 5.

experiencing TFA in domestic and family violence (DFV) situations. This includes where online pornography is a part of children's online experiences, learning, and digital footprint – both within and outside of a context of DFV. It is also used to inform discussions with frontline workers on women's experiences of coercion and sexual violence in DFV, as research suggests this can include the forced watching of pornography and pornography being used as a 'manual' to coerce participation in certain sex acts.[957]

ACWA Resources for Out-of-Home Care Workers

Under eSafety's Online Safety Grants Program, the Association of Children's Welfare Agencies (ACWA) co-designed and developed resources aimed at raising awareness of online safety among children and young people in care and their caregivers.

The resources comprise an online training course and factsheets for caregivers, including in relation to online pornography. The resources also include a series of short videos for children and young people in out-of-home care. [958]

Conclusion

Age-appropriate education about consent, respect, critical thinking, help-seeking, and protective behaviours online is necessary from an early age. It is important to support children and young people in understanding the content they encounter online, including online pornography. Trusted adults should also have the necessary skills and knowledge to discuss online pornography with children.

Any educational approach should consider the changing needs, rights, and best interests of children at different ages and stages. It is important for parents and caregivers to be informed about how to have difficult conversations with children about online pornography.

A whole-school approach to respectful relationships includes a supportive school climate, curriculum, wellbeing teaching and learning activities, staff professional development, student voice and agency, and partnerships with parents, caregivers, and the community. There are

[957] L Tarzi and M Tyler, *'Recognizing Connections Between Intimate Partner Sexual Violence and Pornography',* Violence Against Women, 2021, 27(14):2687–2708. DOI: 10.1177/1077801220971352.

[958] Association of Children's Welfare Agencies Centre for Community Welfare Training, '*ACWA's online safety resources for children and young people in care and their caregivers*', ACWACCWT website, n.d., available at: https://www.acwa.asn.au/esafety-resources/.

several relevant areas of the curriculum where education about online pornography could be integrated.[959]

Stakeholders had different perspectives on when to include pornography-specific education and some schools are hesitant to discuss online pornography due to concerns about appropriateness or student wellbeing.

Teachers and school wellbeing staff often feel unprepared to talk about pornography with students. They need tailored materials to have safe and age-appropriate conversations. Professional development for educators should include information on safety tools to prevent access to online pornography. It should also cover how to integrate discussions about modern online pornography into sex education and respectful relationships topics.

Stakeholders discussed technological approaches to prevent students from accessing pornography at school or on school devices. These include device-level filters, network-level filters, proactive scanning for certain language, and individual incident alerts on the school Wi-Fi network. Robust safety settings and controls in schools will not prevent and address pornography-related incidents at schools and amongst school children. More evidence-based policies, procedures, and resources are needed.

Some young people are critical of how sex and relationships education is delivered. Many see the value in inclusive, stigma-free education. Children and young people want to learn about sex and relationships from their peers. Education should allow for exploration of diverse perspectives in a constructive, trusting, and respectful way. Youth participation and co-design can help make sure messaging is relevant, relatable, authentic, and effective. It can also make sure the content meets young people’s needs.

Children who have experienced instability or uncertainty at home may be more likely to seek support and information from other sources, such as support services. This is compared to children who do not speak English at home. Workers in out-of-home care, youth services, and allied health should be trained to respond to a broad range of online safety issues. eSafety’s resources available for frontline workers could be expanded to include training on the impact and prevalence of online pornography.

Finally, greater coordination across government on intersecting policy developments is required.

[959] The 6th National Survey of Australian Secondary Students and Sexual Health was conducted in 2019. The La Trobe SSS Health Survey was released on December 22, 2022. Studies by M Lim, P Agius, E Carrotte, A Vella, & M Hellard and K Litsou, P Byron, A McKee, and R Ingham discuss young Australians’ use of pornography and its associations with sexual risk behaviours.

Chapter 14 – The Online Safety Act: eSafety's current functions and future opportunities to prevent and minimise harms to children from online pornography

Key points

- The *Online Safety Act 2021* (Cth) (the Act) sets out eSafety's powers and functions, which include:
    - research, education and cross-government coordination relating to online safety
    - operationalising and enforcing the current regulatory frameworks applicable to online pornography, as outlined in the Online Content Scheme, industry codes and/or industry standards, and the Basic Online Safety Expectations.
- The Online Content Scheme is linked with the National Classification Scheme, under which online pornography may be assessed as Refused Classification (RC), X18+ or R18+, depending on the nature of the content. Australia's classification framework is currently under review and any changes will impact the classification of material for the purposes of the Act.
- As provided for under the Act, the eSafety Commissioner declared the Online Safety (Restricted Access Systems) Declaration 2022 ('RAS Declaration 2022') in January 2022. This sets out the minimum requirements that social media services, relevant electronic services and designated internet services provided from Australia must follow to restrict children's access to R18+ content online upon receiving a notice from eSafety.
- Additional requirements can be established through the development of co-regulatory industry codes and/or industry standards under the Online Content Scheme, which could apply to up to eight sections of the online industry and include enforceable measures for relevant participants.
    - **Phase 1** of the industry codes development process is well advanced with five industry codes containing measures to combat content such as child sexual exploitation and pro-terror material registered in May 2022. Phase 1 will likely be complete in the second half of 2023.

  - **Phase 2** will include development of measures aimed at preventing children's access to online pornography.
- The Online Content Scheme offers a strong basis for preventing and mitigating harms to children from online pornography but also presents some challenges. Some of these challenges could be considered in the upcoming review of the Act.
- There is an expectation in place under the Online Safety (Basic Online Safety Expectations) Determination 2022 for social media, relevant electronic and designated internet service providers to take reasonable steps to prevent children's access to online pornography. eSafety will draw on this report to develop any relevant regulatory guidance for services on how they may comply with relevant expectations, and to inform areas that future reporting notices may focus on.

Overview

This chapter outlines eSafety's legislative functions and powers under the Act and how they apply to online pornography. It explains the aspects that have already been put into operation, such as the RAS Declaration 2022, and those under development, including the industry codes. Consistent with the Inquiry Committee's recommendation, it discusses the consultation requirements embedded within each of these elements. The chapter also explores the benefits and challenges of various regulatory options under the Act, and sets out eSafety's intended path forward, noting the Act will be subject to an independent review, to commence by January 2025.

eSafety suggests there are two parts to designing a suitable legislative and regulatory framework and program of consultation for implementing a mandatory age verification regime for online pornography (as requested by the Inquiry).[960]

One part addresses the governance structures and privacy and security protections for such a regime. As discussed in chapter 9, there is substantial work underway to develop such a framework for Australia's Digital Identity system. eSafety proposes this framework – informed by three phases of consultation as well as extensive consultation on the Trusted Digital Identity Framework – could be extended to cover age assurance for online pornography, rather than creating an entirely new framework. Together with the *Privacy Act 1998* (Cth) (Privacy Act) and relevant national strategies and plans, this framework would cover the elements of governance, privacy and security.

[960] House of Representatives Standing Committee on Social Policy and Legal Affairs, '*Protecting the age of innocence: Report of the Inquiry into age verification for online wagering and online pornography*', Parliament of Australia website, 2020.

The second 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. That is the focus of this chapter, which centres on the Act as the existing framework for regulating online pornography and promoting online safety.

eSafety's history, functions and approach

eSafety was established in July 2015 as the Children's eSafety Commissioner. Its original functions under the *Enhancing Online Safety for Children Act 2015* (Cth) included research, education, and a national leadership role in online safety for children. eSafety also administered a regulatory scheme to investigate complaints – and facilitate removal – of child cyberbullying material on social media services.

eSafety was also given responsibility for the Online Content Scheme, then provided for under Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) ('Broadcasting Act'). This included administering a complaints scheme for prohibited online content such as child sexual exploitation material. Accordingly, eSafety took on Australia's membership in the International Association of Internet Hotlines (INHOPE) network, a global network that combats child sexual exploitation material and facilitate its rapid removal.

eSafety also acquired what were then relatively limited powers to require removal or remedial action in relation to online content hosted in Australia. This included requiring some online content found unsuitable for children to be placed behind a 'restricted access system', as defined in the *Restricted Access Systems Declaration 2007* (Cth) made under the now repealed Schedule 5 of the Broadcasting Act. As such, eSafety has been overseeing a basic mandatory age assurance framework since our inception.

In subsequent years, eSafety's remit has been extended to include promoting and improving online safety for Australian adults as well as children. The *Enhancing Online Safety for Children Act 2015* (Cth) became the *Enhancing Online Safety Act 2015* (Cth).

eSafety's functions and powers were broadened to include administration of a civil penalties' regime for the non-consensual sharing of intimate images (also called image-based abuse and sometimes referred to as 'revenge porn'). The evolution also included new powers under the *Criminal Code Act 1995* (Cth) to issue notices to content and hosting services about abhorrent violent material, and a process for blocking websites providing access to certain terrorist content during an online crisis event.

In January 2022, the Act came into effect. It replaced the *Enhancing Online Safety Act 2015* (Cth) as eSafety's enabling legislation and superseded the previous schemes in Schedules 5 and 7 of the Broadcasting Act to address illegal and restricted online content. Its aim is to create a modern, fit-for-purpose regulatory framework that builds on the strengths of the previous legislative schemes for online safety.[961] The Act strengthened and extended eSafety's existing powers and provided new tools to regulate services' online activities and enhance their transparency and accountability.

Section 27 of the Act outlines the legislative functions of eSafety, which amongst other functions, includes a role to:

- support, encourage, conduct and evaluate research about online safety for Australians
- support, encourage, conduct, accredit and evaluate educational, promotional and community awareness programs relevant to online safety for Australians
- make grants of financial assistance in relation to online safety for Australians, including for an individual or a state or territory
- coordinate activities of Commonwealth Departments, authorities and agencies relating to online safety for Australians.

These interrelating functions empower eSafety to provide a holistic approach to online safety issues, including children's access to online pornography. As highlighted in chapter 4, in performing these functions, the Commissioner must, as appropriate, have regard to the Convention on the Rights of the Child.[962]

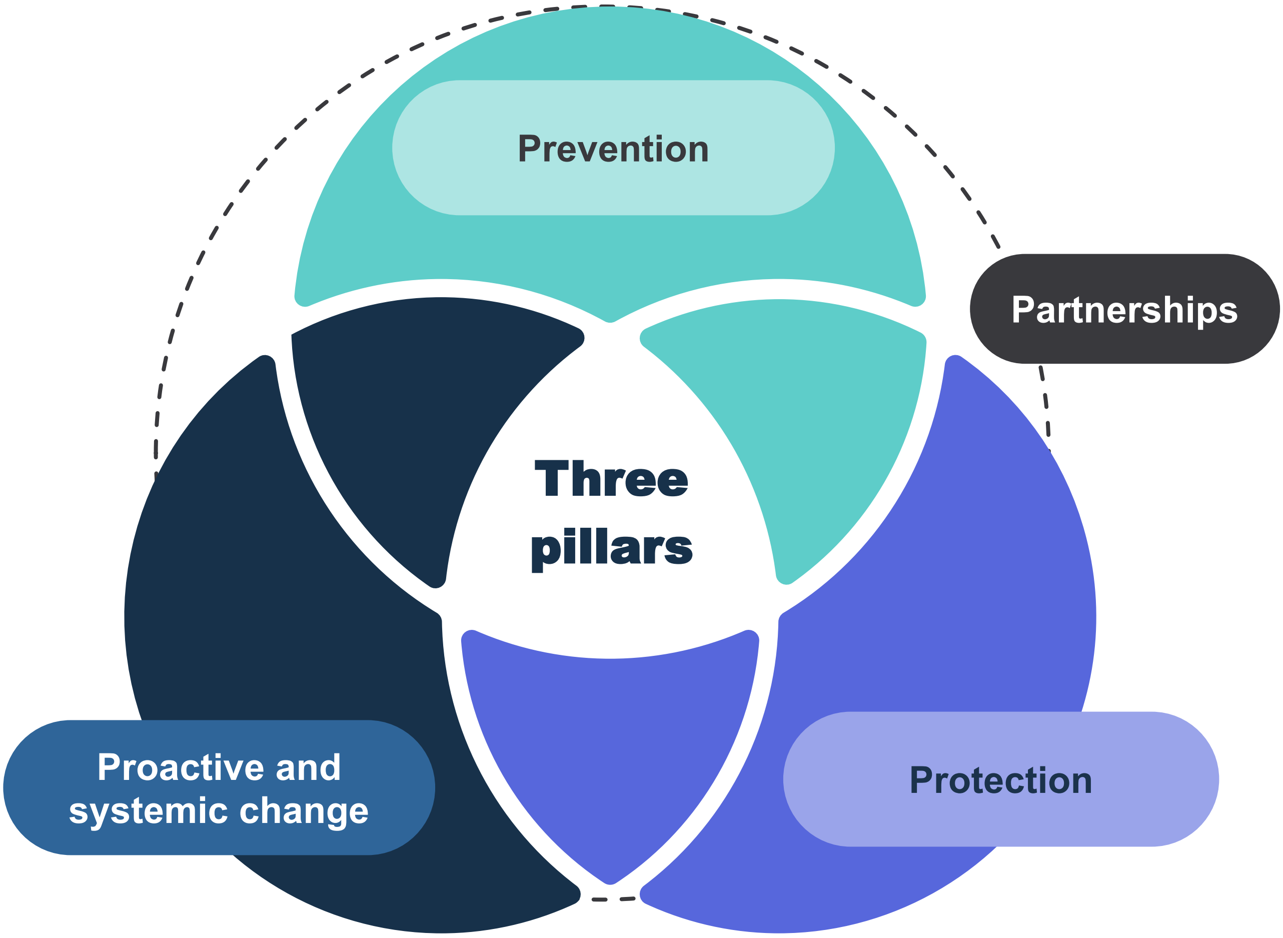
eSafety's purpose is to safeguard Australians at risk from online harms and promote safer, more positive online experiences through three connected pillars: prevention, protection and proactive change.

- **Prevention** - eSafety conducts research and provides evidence-based online safety resources and programs which empower individuals, families and communities to be safer online. Our research is referenced throughout this report, particularly in chapter 5, and our education initiatives are explored in chapter 13.
- **Protection** - eSafety operates regulatory schemes and takes action to address complaints from the public about cyberbullying of children, adult cyber abuse, image-based abuse and other forms of illegal and restricted online content discussed in this chapter.
- **Proactive and systemic change -** eSafety engages in consultation and environmental and horizon scanning to understand existing and emerging online threats. We promote safety, transparency and accountability through new reporting powers, as well as through the

[961] Parliament of Australia, '*Online Safety Bill 2021 – Explanatory Memorandum'*, Parliament of Australia website, 2021, available at: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.

[962] United Nations, '*Convention on the Rights of the Child',* available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

provision of voluntary guidance material and tools, notably Safety by Design[963]. We develop these tools with industry to enable providers of products and services to lift safety capabilities to better protect their customers' safety and rights. eSafety also has powers through industry codes and/or standards to require industry to take steps to limit the availability of illegal and restricted online content.



[963] Online Safety Act 2021 (Cth), s 24.

How the Online Safety Act applies to pornography

Online content regulated under the Act ranges from material of the highest and most serious harm, such as videos of the sexual abuse of children or terrorism, to material which can be harmful for children, such as online pornography.

Referred to as 'class 1' and 'class 2', this material is subject to the Online Content Scheme in Part 9 of the Act.[964] This Scheme also contains powers that allow eSafety to give enforceable notices that direct online service providers to take reasonable steps to remove or restrict access to this material on their services.

Class 1 and class 2 material

Class 1 and class 2 material are defined under the Act by reference to the National Classification Scheme, a cooperative arrangement between the Australian Government and state and territory governments for the classification of films, publications and computer games.[965]

The National Classification Scheme is implemented through the *Classification (Publications Films and Computer Games Act 1995* (Cth) (Classification Act)[966] and complementary state and territory enforcement legislation. This complementary legislation sets out how films, publications and computer games can be sold, hired, exhibited and advertised in each state or territory.

Offences relating to class 1 and class 2 material

- State and territory legislation provides for offences in relation to selling, screening, distributing or advertising various categories of classified material (or material that, if classified, would be classified as being in a certain category). State and territory agencies are responsible for enforcement of these laws.
- Offences vary significantly across Australian states and territories. While all jurisdictions ban the possession of child sexual exploitation material, the treatment of other types of material is varied. Mere possession of some other forms of Refused Classification (RC) material can be an offence (for example, instructions for manufacturing drugs). However, in most jurisdictions, possession of Refused

[964] eSafety Commissioner, *'Online Content Scheme: Regulatory Guidance',* eSafety website, 2021.
[965] Online Safety Act 2021 (Cth), s 106-107.
[966] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, '*Australian Classification (Publications, Films and Computer Games) Act 1995*', available at: https://www.classification.gov.au/about-us/legislation.

Classification (RC) material (other than child sexual exploitation material) is only an offence where there is an intent to sell or exhibit the material.

- The sale or distribution of X18+ films is illegal in most of Australia (except in ACT and NT), though viewing and possession for personal use is not an offence. It is not an offence in any state or territory to possess R18+ material.

The Classification Act establishes the Classification Board and Classification Review Board and sets out their responsibilities and procedures for decision-making. The Classification Act is supplemented by several regulations, determinations and legislative instruments, including the *National Classification Code (May 2005)* (Cth) (National Classification Code), *Guidelines for the Classification of Publications 2005* (Cth*)*, *Guidelines for the Classification of Films 2012* (Cth*)* and *Guidelines for the Classification of Computer Games 2012* (Cth*)*. These provide the principles and criteria for making classification decisions.

National Classification Code

- Under the National Classification Code, classification decisions are to uphold the following principles:
  - Adults should be able to read, hear, see and play what they want
  - Minors should be protected from material likely to harm or disturb them
  - Everyone should be protected from exposure to unsolicited material they find offensive.
- The need to take account of community concerns about:
  - depictions that condone or incite violence, particularly sexual violence
  - the portrayal of persons in a demeaning manner.
- Under the Act, **class 1** and **class 2** content is defined by reference to:
  - The classification it has received by the Classification Board under the Classification Act (where the material has been classified)
  - eSafety's assessment of the classification the material would likely be given by the Classification Board under the Classification Act and the classification guidelines for films (where the material has not been classified).[967]

[967] Online Safety Act 2021 (Cth), s 106.

Pornography is not a distinct category of material under the classification regime. Instead, online pornography could be classified as RC, X18+ or R18+, depending on what it contains and its potential impact, such as where content is detailed, accentuated, or uses specific effects, prolonged, repeated frequency, realistic or encourages interactivity.

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.

Review of Australian classification regulation and stakeholder feedback

The National Classification Code and the guidelines for the classification of films, computer games and publications were designed primarily to assess commercially produced material before its release into the community.

They focus on content that may be offensive, more than harmful. They also treat certain categories of behaviour, including specific fetish practices within pornography, as inherently offensive.

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.[968] This review sought to develop a classification framework that meets community needs and reflects today's digital environment. The review was released on 29 March 2023 and the Government announced its intention to reform the National Classification Scheme.

During eSafety's consultations for this report, 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, and its potential to stigmatise and censor queer sex practices and content, as an example.[969]

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.[970]

Some stakeholders also highlighted the inconsistency between the age to access to pornography (18) and the age of consent to sex (generally 16 or 17 depending on the state or territory).[971] They felt the age of consent could be used to guide the age of access to online pornography. This was echoed in eSafety's focus groups with 16-18-year-olds. As discussed in chapter 10, the current age differential may create challenges in immersive environments, where the lines between pornography as online content versus pornography as sexual activity may be blurred.

Considering these issues, some stakeholders suggested postponing implementation of the age verification roadmap until after the classification review is completed.[972]

Future directions

Section 239A of the Act provides that the Minister for Communications should cause an independent review of the Act to be initiated within 3 years after its commencement. The government's response to the House of Representatives' Select Committee *Inquiry into Social Media and Online Safety* indicated that the review of the Act will commence prior to the next election. eSafety suggests that any outcomes from the classification regulation review, and their potential implications for the Online Content Scheme, should be considered when this review of the Act is conducted.

[968] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, '*Review of the Australian classification regulation*', DITRDCA website, 2020.
[969] See Appendix 5, p14.
[970] See Appendix 5, p13.
[971] Australian Institute of Family Studies, *'Age of consent laws in Australia',* AIFS website, 2021, available at: https://aifs.gov.au/resources/resource-sheets/age-consent-laws-australia
[972] Online Safety Act 2021 (Cth), Part 9.

Powers under the Online Content Scheme

The Online Content Scheme within Part 9 of the Act replaced the previous schemes in Schedules 5 and 7 of the Broadcasting Act to address illegal and restricted online content meeting the definition of class 1 or class 2 material.

As noted above, online pornography may fall within either class 1 or class 2, depending on the nature of the content.

Class 1 material powers

While some forms of online pornography depicting fetishes or violence fall within the definition of class 1 material, at the core of this category – and of highest concern to eSafety – is child sexual exploitation material and material advocating terrorism.

The Online Content Scheme provides eSafety with a range of powers in relation to class 1 material (in addition to industry codes and standards discussed later in this chapter).[973] These include:

- assessing whether material that can be accessed by end-users in Australia is considered class 1, either on our own initiative or in response to complaints from the public
- a removal notice requiring the provider of a social media service, a relevant electronic service, a designated internet service, or a hosting service provider to take all reasonable steps to remove or cease hosting class 1 material that can be accessed by end-users in Australia
- a link deletion notice requiring the provider of an internet search engine service to cease providing a link that can be used by end-users in Australia to access class 1 material.
- an app removal notice requiring the provider of an app distribution service to cease enabling end-users in Australia to use the service to download an app that facilitates the posting of class 1 material on a social media service, a relevant electronic service, or a designated internet service
- formal enforcement actions, including formal warning, enforceable undertaking, injunctions, civil penalty orders, and referral of matters to law enforcement.

As set out in our regulatory guidance,[974] in determining whether to take action, eSafety considers:

[973] Online Safety Act 2021 (Cth) Part 9.
[974] eSafety Commissioner, *'Online Content Scheme: Regulatory Guidance',* eSafety website, 2021, available at: https://www.esafety.gov.au/sites/default/files/2021-12/eSafety-Online-Content-Scheme.pdf.

- the harm or likely harm from production of the material (for example, to victims of child sexual exploitation or violent crime)
- the harm or likely harm from consumption of the material (for example, normalising child sexual exploitation by allowing access to and sharing of images and videos of children being sexually abused)
- whether other options exist to limit access to the material (for example, device-level filtering software or parental control tools)
- the context in which the material is presented (for example, content that is presented in a factual and object way intended to contribute to public debate may be regarded as having a lower impact than the same material presented without contextual justification) and
- any other factors that eSafety considers to be of relevance.

eSafety prioritises the investigation of complaints about the most harmful class 1 material. Of the investigations we carry forward from these complaints, 99% concern child sexual exploitation material. All but a handful of these are notified to the International Association of Internet Hotlines (INHOPE) network for rapid removal within the host jurisdiction.[975] Because our work with INHOPE provides a highly effective pathway for takedown, eSafety rarely needs to consider formal regulatory action in relation to child sexual exploitation material. 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) to focus our resources on the removal of the highest harm form of online content, such as pro-terror and child sexual exploitation material.

While eSafety's removal powers offer an important safety net, they are only capable of actioning content on a case-by-case basis. That is why the Act also establishes new options to regulate services' broader systems and processes, including the development of industry codes or standards and the determination of the Basic Online Safety Expectations.

Class 2 material powers

Class 2 material captures content that may be harmful to children, including online pornography, as well as material containing high impact depictions of violence or drug use.

[975] Parliament of Australia, *'Submissions to the Inquiry on law enforcement capabilities in relation to child exploitation'*, 2023, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation47th

eSafety's removal and remedial powers under the Online Content Scheme in relation to class 2 material are more limited, and only apply to content on a social media, relevant electronic or designated internet service provided from or hosted in Australia. The Act does not provide eSafety with removal powers in relation to overseas-hosted class 2 material. Class 2 material is almost entirely hosted overseas.

Where the content is likely to amount to X18+ material, and is provided from Australia, eSafety can issue a removal notice.[976]

Where the content is likely to amount to R18+ material, and is provided from Australia, eSafety can issue a remedial notice.[977] This requires the provider to take all reasonable steps to ensure the material is removed (or its hosting ceased) or placed behind a 'restricted access system'.

Restricted Access System

A restricted access system (RAS) is an access-control system that meets the requirements set out in the RAS Declaration 2022. In determining these requirements, the eSafety Commissioner was required to have regard to particular matters, including the objective of protecting children from exposure to material that is unsuitable for them.[978] Specifically, it applies for the purposes of assessing regulatory action to be taken in relation to material provided from Australia that has been or is likely to be classified R18+ under the National Classification Code. The eSafety Commissioner made the relevant declaration in January 2022 which identifies the features of a RAS.[979]

Development of the current RAS Declaration

The first declaration relating to restricted access systems, the (*Restricted Access Systems Declaration 1999 (No. 1)* (Cth*)*, was made in 1999 under subclause 4(1) of Schedule 5 of the Broadcasting Act. It was then repealed in January 2008 following the repeal of subclause 4(1).

The *Restricted Access System Declaration 2007* (Cth*)* took effect in February 2008 and was replaced in 2014 by the *Restricted Access Systems Declaration 2014* (Cth*)* (2014 RAS Declaration).

In August 2021, eSafety facilitated an initial consultation on the RAS for the purposes of the Act. We sought views of the online industry and the wider community on a consultation paper about the effectiveness of the RAS arrangements established in 2007 and updated in 2014. We also sought views on the administrative and financial burden of implementing a RAS, and design elements of a new RAS framework.[980] As noted in chapter 3, given the close relationship

[976] Online Safety Act 2021 (Cth), s 114-115.
[977] Online Safety Act 2021 (Cth), s 119-120.
[978] Online Safety Act 2021 (Cth), s 108.
[979] Online Safety (Restricted Access Systems) Declaration 2022.
[980] eSafety Commissioner, *'Age verification'*, eSafety website, n.d., available at: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification.

between the age verification roadmap and the RAS framework, eSafety began these processes concurrently.

eSafety received a range of submissions from a cross-section of online services, NGO and advocacy groups, academia and community members. Themes from these submissions included the need for flexibility, the requirement for privacy-preserving technologies, issues faced by sole traders, and the need to exclude sexual health information and educational resources from the scope of class 2 material.

In October 2021, consistent with requirements of the *Legislation Act 2003 (*Cth*)*, a draft RAS instrument and Explanatory Statement were released for public consultation.[981] eSafety received 31 submissions, mostly from stakeholders of the initial consultation who were supportive of the draft instrument. The final RAS Declaration 2022 was registered and took effect in January 2022 with the commencement of the Act.[982] The instrument is set to sunset on 1 April 2032.

RAS Declaration in practice

Like the 2014 RAS Declaration, the current RAS Declaration does not specify or prescribe technologies or processes to be used by service providers to determine age and restrict access to content.

The RAS Declaration states that an access-control system must:

- require an application be made by a person in order to access to the relevant class 2 material. This application must include a declaration in writing or electronic form that the applicant is at least 18 years of age
- give warnings about the nature of the material and safety information about how a parent or guardian may control access to the material
- incorporate reasonable steps to confirm an applicant is at least 18 years of age
- limit access to the material unless certain steps are followed.[983]

The RAS Declaration's Statement of Compatibility with Human Rights notes that providers must continue to comply with their obligations under applicable privacy laws, such as the Privacy Act,

[981] eSafety Commissioner, *'Draft RAS declaration',* eSafety website, 2021; eSafety Commissioner, Explanatory Statement – Restricted Access Systems Declaration 2021, eSafety website, 2021, available at: https://www.esafety.gov.au/sites/default/files/2021-10/Draft explanatory statement framework of the RAS Declaration 2021.pdf.

[982] Online Safety (Restricted Access Systems) Declaration 2022.

[983] eSafety Commissioner, *'Restricted Access System Declaration – Online Safety Act 2021: Discussion Paper'*, eSafety website, 2021, available at: https://www.esafety.gov.au/sites/default/files/2021-08/OSA - Restricted Access System discussion paper_0.pdf.

discussed in chapter 9, and that a data minimisation approach should be taken to ensure the only attribute being tested is the age of the applicant.[984]

Application of the RAS

At the time of delivering the Roadmap to government, eSafety has not issued a remedial notice under the Online Safety Act directing a service either to place content behind a RAS or to remove it. In a situation where eSafety received a report of 'unrestricted' (i.e., not behind a restricted access system) class 2 content provided from Australia (depicting a violent fight, as opposed to pornography), eSafety made an informal request for the video to be restricted or removed. The video was removed by the platform and the account was suspended.

Several organisations have adjusted their practices in response to the RAS Declaration. For example, as noted in chapter 8, Google has introduced new age assurance steps on YouTube and Google Play, which require some Australian users to provide additional proof of age when attempting to watch mature content on YouTube or downloading content on Google Play.[985] The Scarlet Alliance and Eros have also developed information resources and guidance for their members in relation to the RAS and its requirements.[986]

Future directions

As outlined in the Explanatory Statement to the RAS Declaration[987], the non-prescriptive approach of the RAS Declaration is intended to:

- protect children from exposure to unsuitable content without imposing unreasonable financial or administrative burden on service providers
- give service providers flexibility to implement restriction measures that reflect the nature of their services, their business models, and their size, capacity, capability and maturity
- allow for advances in relevant technologies.

Following extensive research and consultation for this report, eSafety believes more detailed age assurance and complementary safety requirements for providers could be implemented while still achieving these goals of flexibility and innovation.

[984] Online Safety (Restricted Access Systems) Declaration 2022.
[985] Google Australia, '*Ensuring Age Appropriate Experiences*', Google website, 2022, available at: https://blog.google/intl/en-au/company-news/technology/ensuring-age-appropriate-experiences/.
[986] Scarlett Alliance, *'Scarlet Alliance Community Policy Kit – Write Your Own Submission on the new Online Safety Bill, Scarlett Alliance website'*, 2020, available at: https://scarletalliance.org.au/wp-content/uploads/2022/07/online_safety_bill_2020.pdf.
[987] Online Safety (Restricted Access Systems) Declaration 2022.

While further requirements could be set through the development of a new RAS Declaration, eSafety does not view this as the most effective avenue. Under the Act, the RAS Declaration only applies for the purposes of regulating access to R18+ content provided from Australia. A large proportion of mainstream pornography is likely to constitute X18+ or RC content and is often provided from outside Australia. The Commissioner can require that material classified as (or likely to be classified as) X18+ or RC be removed but cannot require that it be placed behind a RAS. Therefore, a new RAS Declaration would have limited applicability. eSafety suggests the scope of content and services subject to the RAS Declaration could be considered when the Act is reviewed. Industry codes or standards, which apply to a much broader range of online content and service providers across the globe, would be the preferred avenue for these measures.

To prevent any inconsistency between what a service provider might be required to do under the RAS Declaration and an industry code or standard, eSafety believes the RAS should be considered as setting the baseline requirements for social media services, relevant electronic services, and designated internet services. Any further measures established through industry codes or standards could be built on top of – and consistent with – the RAS's four key components.

Industry codes or standards

While the class 1 and class 2 removal and remedial powers can serve as a safety net to address individual items of content, the Act also provides important new channels for eSafety to regulate online services' systems and processes, based in part on systemic issues identified through our individual complaints schemes. One such channel is the development of industry codes or industry standards.

Industry codes

The Act provides for industry bodies or associations to develop new codes to regulate class 1 and class 2 material, and for eSafety to register the codes if they meet certain statutory requirements, including provision of appropriate community safeguards.[988]

The purpose of the codes is to create a modernised, co-regulatory response across the whole digital ecosystem.[989] This includes eight key sections of the online industry: social media services, relevant electronic services, designated internet services, hosting services, search engines, app distribution services, ISPs, and manufacturers, suppliers and installers of equipment.[990]

Compliance with applicable codes is mandatory for those who fall within these categories and, for seven of the eight sections of the online industry, those who provide services or equipment to end-users in Australia.[991] A code covering hosting services would apply to the extent that the services host material in Australia.

Industry standards

Where certain conditions are met, the Commissioner may determine an industry standard, which is a legislative instrument determined by the eSafety Commissioner rather than by industry. There are three main scenarios in which an industry standard can be developed, each with its own requirements to be met before it can be relied upon:

- If the Commissioner requests that an industry body or association develop an industry code and the request is not met, or the Commissioner determines that the code does not provide appropriate community safeguards or does not meet relevant targets specified in the request, or the Commissioner otherwise refuses to register the code

[988] Online Safety Act 2021 (Cth), Part 9 Division 7.
[989] Online Safety Bill 2021 – Explanatory Memorandum.
[990] Online Safety Act 2021 (Cth), s 135.
[991] This only applies to equipment for use to access services on the internet which constitutes: a social media service, a relevant electronic service, a designated internet service, or an internet carriage service.

- If there is no industry association to represent the relevant industry section and none comes into existence within a specified period
- If an industry code has been developed and registered by the Commissioner but, after at least 180 days of its operation, the Commissioner is satisfied that the code is deficient after giving industry the opportunity to address specified deficiencies.[992]

Industry codes or standards subject matter

The industry codes or standards may apply to matters relating to the online activities of industry participants that deal with online safety and content issues.

Section 138(3) of the Act includes a list of examples of matters that may be dealt with by the industry codes or industry standards. These include procedures for dealing with class 1 material or class 2 material, providing users with access to technological solutions to limit access to class 1 and class 2 material, and providing users with advice on how to limit access to class 1 and class 2 material. Notably, these examples do not limit the matters that may be dealt with by the industry codes or standards.

Enforcement

eSafety can receive complaints[993] and investigate potential breaches of the codes or standards[994], and they will be enforceable through civil penalties, infringement notices, enforceable undertakings and injunctions.[995]

Section 144 of the Act empowers the Commissioner to issue a formal warning to an industry participant contravening a registered code that applies to them. Similarly, section 147 empowers the Commissioner to issue a formal warning in relation to the breach of an industry standard that applies.

Section 143 provides that, where the Commissioner is satisfied an industry participant has contravened or is contravening a registered code applying to them, the Commissioner may direct that industry participant in writing to comply with the code. Section 146 requires that an industry participant comply with an industry standard that applies to them. Failure to comply with a written direction under section 143 and failure to comply with an industry standard both give rise to a civil penalty of 500 penalty units.

[992] Online Safety Act 2021 (Cth), s 145.
[993] Online Safety Act 2021 (Cth), s 40.
[994] Online Safety Act 2021 (Cth), s 42.
[995] Online Safety Act 2021 (Cth), Part 10.

Civil penalties under the Act are enforceable under Part 4 of the Regulatory Powers (Standard Provisions) Act 2004 (Cth). Respondents under the Act may face civil penalties of up to $156,500 units for an individual and up to $782,500 for a body corporate.[996]

Industry codes development process to date

In September 2021, eSafety published a position paper setting out expectations about the scope of the codes, as well as proposed objectives, outcomes and example measures.[997] eSafety commenced working with industry in early 2021 to on the development of codes which informed its position paper.

eSafety proposed a phased approach to the code development process. Phase 1 included codes to be developed for the most harmful class 1 material, including child sexual exploitation material, pro-terror and extreme content, crime and violence. Phase 2 would then seek to address children's access to all forms of online pornography, informed by this report, and other high impact content.

Phase 1

In 2021, a steering group of six industry associations formed and engaged with eSafety to develop these codes covering the eight sections of industry. Those associations are:

- Australian Mobile Telecommunications Association
- BSA | The Software Alliance
- Communications Alliance Ltd
- Consumer Electronics Suppliers Association
- Digital Industry Group Inc
- Interactive Games and Entertainment Association

The Steering Group adopted the suggested phased approach and began developing a set of codes to apply to child sexual exploitation material, pro-terror and extreme content, crime, drug-related content and violence.

In April 2022, eSafety issued notices to members of the Steering Group under section 141 of the Act, formally requesting their development of Phase 1 codes, with a submission deadline of 9

[996] From 1 July 2023, the value of a single penalty unit is $313. Section 82(5) of the Regulatory Powers (Standard Provisions) Act 2014 provides that the maximum pecuniary penalty that can be ordered by a court for a body corporate is 5 times the pecuniary penalty specified for the civil penalty provision. For an individual, the maximum amount is the amount specified for the civil penalty provision.

[997] eSafety Commissioner, '*Development of industry codes under the Online Safety Act: Position paper*', eSafety website, 2021, available at: https://www.esafety.gov.au/sites/default/files/2021-09/eSafety Industry Codes Position Paper.pdf.

September 2022. The issue of these notices created a clear deadline for the submission of codes. Failure to comply with the notice would enliven the Commissioner's power to determine industry standards. These notices were formally varied in June 2022, extending the submission deadline to 18 November 2022.

The Steering Group and industry participants worked closely with eSafety, through exchanges of drafts and written feedback, along with formal meetings, throughout 2022 and early 2023.

The Act requires industry associations to consult with members of the public, the relevant sections of the online industry and the Commissioner.[998] Public consultation took place in September 2022, with 88 submissions received from organisations and members of the public.[999]

Relevant issues raised in some of these submissions include the appropriateness of categorising pornography as class 1 material, the effectiveness of mainstream age assurance techniques such as date of birth self-declarations, as well as the suitability and applicability of the UK Children's Code ('Age Appropriate Design Code') in an Australian context.

As part of this process, the Steering Group also commissioned consumer research, which has been cited in this report and held an expert roundtable.[1000]

The draft codes for eight industry sections were submitted to eSafety for consideration in November 2022. In February 2023, the Commissioner wrote to the relevant industry associations to provide preliminary views of the draft codes, noting they were unlikely to provide the appropriate community safeguards required to be registered. Industry associations were asked to respond to specific areas of concern and/or submit revised codes with improved protections by 9 March 2023. In response to request from industry associations for additional time to respond, the Commissioner granted an extension till 31 March 2023.

The Commissioner found five of the submitted codes satisfied the statutory requirements for registration. They were registered on 16 June 2023 and will come into effect on 16 December 2023.[1001] The Commissioner reserved her decision on one code and requested amendments to address risks associated with recent development in the integration of generative artificial intelligence into search engines. A revised code was submitted to eSafety for registration in July 2023. This is currently under consideration. The Commissioner found two of the submitted codes did not meet the statutory requirements and will determine industry standards for those

[998] Online Safety Act 2021 (Cth), s 140.

[999] Online Safety, *'Industry Codes public consultation'*, n.d., https://onlinesafety.org.au/

[1000] Online Safety, 'Industry Codes public consultation submissions', n.d., https://onlinesafety.org.au/submissions/

[1001] eSafety Commissioner, '*Register of industry codes and industry standards for online safety*', available at: https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards two industry sections. The Commissioner will consult publicly during a standard development process.[1002]

Phase 2

A key purpose of Phase 2 codes is to prevent and address the harms to children associated with accessing online pornography. Accordingly, this is a logical avenue for implementing some of the recommendations from this report, aligning with the basic RAS requirements, and incorporating further good practice measures identified through our consultations and research.

Development of Phase 2 codes is expected to commence after industry codes and/or standards are in place for Phase 1. Chapter 12 outlines a range of measures which could be considered for preventing and addressing the harms to children associated with accessing online pornography.

There are some potential challenges which will need to be considered and addressed with stakeholders:

- One challenge of the co-regulatory process is that the major online services whose primary purpose is providing pornography (set out in chapter 6) do not currently appear to have a representational industry association to develop an industry code on their behalf. There are associations which represent the local adult industry that contributed to consultation processes for this report, including Eros Association, Australia's longest serving adults-only industry association, and Scarlet Alliance, the national peak body representing sex workers and sex worker organisations and projects in Australia. Whether these associations, the associations engaged in Phase 1, other bodies, or a combination thereof, could be capable of representing one or more sections of the online industry for purposes of Phase 2 codes is a matter for consultation and consideration at the conclusion of Phase 1.
- Another challenge is public criticism of the co-regulatory model, and the Act's requirement that the online industry be given an opportunity to develop codes for themselves rather than eSafety having the power to proceed directly to industry standards. For example, Reset Australia published a research report in December 2022 arguing that co-regulation does not meet community expectations, leads to weaker protections, and may not be appropriate in the context of the Online Content Scheme given the level of risk technology creates.[1003]

eSafety and the online industry will need to consider the stakeholder views raised and the lessons learned from the Phase 1 code process to inform Phase 2 developments.

[1002] Online Safety Act 2021 (Cth), s 148.
[1003] Reset Australia, *'How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot'*, Reset Australia website, 2022, available at: https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/.

Service provider determinations

In addition to industry codes and standards, the Online Content Scheme provides a framework for the development and enforcement of service provider determinations.[1004] This empowers the eSafety Commissioner to determine, by legislative instrument, rules that apply to providers of social media services, relevant electronic services, designated internet services, hosting services, and internet carriage services and their respective services.[1005]

For the Commissioner to exercise this power, the Minister for Communications must have first made legislative rules under section 240 of the Act. This is because a service provider determination must relate to a matter specified in the legislative rules.[1006] The Minister also has the power under the Act to determine that specified providers are exempt from service provider determinations or a specified service provider determination.[1007]

If a provider of a service has contravened or is contravening a service provider rule that applies to them (created through a service provider determination), the eSafety Commissioner may give that person a formal warning[1008] or a written remedial direction that requires the provider to take specified action directed towards ensuring future compliance with the service provider rules.[1009]

Non-compliance with the rules is a contravention of a civil penalty provision which may result in a court-imposed financial penalty against the non-complying service provider, [1010] but cannot be subject to an infringement notice or enforced through an injunction or enforceable undertaking.[1011]

Future directions

To date, the Minister has not made any legislative rules. If the Minister were to make legislative rules dealing with relevant matters, making service provider determinations may be an option for the Commissioner. However, this is ultimately a matter for the Minister to decide and the extent to which the legislative rules may address relevant matters is a determination for the Minister to make.

If legislative rules dealing with relevant matters were to be made, eSafety would only recommend the use of service provider determinations if the outcomes achieved through

[1004] Online Safety Act 2021 (Cth), Part 9, Division 8.
[1005] Online Safety Act 2021 (Cth), s 151(1).
[1006] Online Safety Act 2021 (Cth), s 151(4).
[1007] Online Safety Act 2021 (Cth), s 152.
[1008] Online Safety Act 2021 (Cth), s 155.
[1009] Online Safety Act 2021 (Cth), s 154.
[1010] Online Safety Act 2021 (Cth), s 153, 162.
[1011] Online Safety Act 2021 (Cth), 10.

industry codes and standards were deemed unsuitable. The development of any legislative rules would need to involve appropriate and reasonably practical consultation process as required by Section 17 of the *Legislation Act 2003* (Cth) and would be subject to the usual parliamentary scrutiny processes for delegated legislation.

Powers to seek a Federal Court order

The Online Content Scheme also provides eSafety with powers to seek a Federal Court order to stop the provision of a social media service, relevant electronic service, designated internet service or internet carriage service in certain circumstances.[1012] These powers have not yet been exercised by eSafety.

Before applying for such an order, the Commissioner must be satisfied there were two or more occasions during the previous 12 months on which the provider of the service contravened a civil penalty provision under the Online Content Scheme, and as a result of those contraventions, the continued operation of that service represents a significant community safety risk.[1013]

Future directions

Requirements to comply with industry standards, service provider rules, and written directions to comply with industry codes constitute civil penalty provisions. Therefore, repeated non-compliance with age assurance and complementary safety measures required under these instruments could result in the Commissioner considering whether the continued operation of the service represents a significant community safety risk such that an application for a Federal Court order is warranted.

However, we note similar court processes in other jurisdictions have lasted many years, including Germany and France. When the Act is reviewed, consideration could be given to providing eSafety with additional powers to address instances where repeat contraventions have created significant risks for children. One such power could include ISP blocking, which is currently available to the regulator in Germany, discussed in chapter 10.

[1012] Online Safety Act 2021 (Cth), Part 9, Division 9.
[1013] Online Safety Act 2021 (Cth), ss 156-159(1).

ISP blocking

Currently, eSafety's power to request or require ISP blocking may be used only in relation to material that depicts, promotes, incites or instructs in abhorrent violent conduct such as murder, rape, kidnapping or terrorist acts, where the availability of that material is likely to cause significant harm to the Australian community.[1014] The intent of this power is to prevent the rapid distribution of terrorist and extreme violent material online, as occurred, for example, after the 2019 terrorist attacks in Christchurch, New Zealand.[1015]

As the purpose is to provide a rapid response to such material, the Commissioner is not required to observe any requirements of procedural fairness in relation to giving a blocking request or notice.[1016] However, the initial blocking period cannot exceed three months,[1017] and the Commissioner must notify the person to whom the relevant domain name is registered as soon as practicable.[1018] In addition, the Commissioner is required to consider whether any other, less restrictive powers could be used to minimise the likelihood that the availability of the material online could cause significant harm[1019] and the decision to give a blocking notice may be subject to internal review by eSafety or external review by the Administrative Appeals Tribunal.[1020]

The review of the Act could consider the appropriateness and extent to which eSafety could exercise an additional ISP blocking power for circumstances where services are providing children with access to online pornography. The provision of such notices could be limited to circumstances where services have not implemented age verification or assurance measures. The decision to issue such notices could also be subject to other protections, including procedural fairness requirements and rights of review. Any amendments to the Act to enable this kind of change would also be subject to the usual scrutiny of amendments to legislation including a regulatory impact assessment, consultation, assessment of compatibility with human rights and parliamentary scrutiny.

[1014] Online Safety Act 2021 (Cth), Part 8.
[1015] Online Safety Bill 2021 – Explanatory Memorandum.
[1016] Online Safety Act 2021 (Cth), ss 95(3), 99(3).
[1017] Online Safety Act 2021 (Cth), ss 96, 100.
[1018] Online Safety Act 2021 (Cth), ss 98, 102.
[1019] Online Safety Act 2021 (Cth), ss 95(5), 99(5).
[1020] eSafety Commissioner, *'Online Safety (Internal Review Scheme) Instrument 2022 (Cth) s5(2)'*, available at: https://www.esafety.gov.au/sites/default/files/2022-01/Online%20Safety%20%28Internal%20Review%20Scheme%29%20Instrument%202022.pdf; Online Safety Act 2021 (Cth) s220 (13).

Basic Online Safety Expectations

Another important new avenue under the Act for the regulation of some online services is the power for the Minister to set online safety expectations for service providers called the Basic Online Safety Expectations (the Expectations).[1021]

What is included in the Expectations?

The *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth*)* (Determination) in January 2022, is a mechanism for the Minister to articulate expectations that social media services, relevant electronic services and designated internet services, will take steps to meet those expectations to protect Australians from unlawful and harmful material and activity that falls within the remit of the Act or impedes the online safety of Australians.[1022]

The Department of Infrastructure, Transport, Regional Development and Communications publicly consulted on a draft Determination, with 62 submissions from interested stakeholders.[1023]

Under the Act, eSafety is provided with powers to issue notices to providers requiring them to report on their implementation of the Expectations. This is intended to promote transparency and accountability from industry and incentivise improvements in safety standards.

The Expectations establish, amongst other things, that providers should:

- take reasonable steps to ensure end-users can use their service in a safe manner, including by proactively minimising the extent to which material or activity on the service is unlawful or harmful[1024]
- take reasonable steps to minimise the provision of certain material, including class 1 material, cyberbullying and cyber-abuse material, non-consensual intimate images, and material relating to abhorrent violent conduct[1025]
- take reasonable steps to ensure that technological or other measures are in effect to prevent access by children to class 2 material provided on the service[1026]

[1021] Online Safety Act 2021 (Cth), Part 4.
[1022] Australian Government, *'Explanatory Statement to the Online Safety (Basic Online Safety Expectations) Determination 2022*', available at: https://www.legislation.gov.au/Details/F2022L00062.
[1023] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, '*Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation*', DITRDCA website, 2021, available at: https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.
[1024] Online Safety (Basic Online Safety Expectations) Determination 2022 (Determination), section 6.
[1025] Online Safety (Basic Online Safety Expectations) Determination 2022 (Determination), section 11.
[1026] Online Safety (Basic Online Safety Expectations) Determination 2022 (Determination), section 12(1).

- ensure the provider has clear and readily identifiable mechanisms that enable end-users to report, and make complaints about, certain material provided on the service[1027]
- ensure the service has terms of use and policies and procedures in place in relation to the safety of end-users, that there are clear and readily identifiable mechanisms to report and complain about breaches of the terms of use, and that penalties are enforced against all accounts who breach the terms of use.[1028]

In some areas, the Expectations provide examples of what reasonable steps might look like for providers. Subsection 12(2) states that reasonable steps to ensure children do not access class 2 material could include implementing age assurance mechanisms and conducting child safety risk assessments. Additionally, the Expectations set out that robust and restrictive default privacy and safety settings for children is an example of reasonable steps that can be taken to ensure safe use of a service.

Compliance with the Expectations is not enforceable via proceedings in a court or under the *Regulatory powers (Standard Provisions) Act 2014* (Cth), but 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 notice or determination. Reporting can be required on either a one off ('non-periodic') or regular ('periodic') basis.

Additionally, the eSafety Commissioner may make a 'service provider notification' if a provider has contravened one or more of the Expectations that apply to it, or if the provider has complied with all of the Expectations. The intention of this is to introduce a reputational risk for non-compliance and positive reinforcement for complete compliance to incentivise providers.[1029]

Implementation of Expectations

The Expectations came into effect on **24 January 2022**.

On 29 August 2022, the eSafety Commissioner issued non-periodic reporting notices to seven providers (Meta and WhatsApp, Apple, Microsoft and Skype, Snap and Omegle) with questions about what steps these providers are taking to implement the Expectations on their platforms, specifically in relation to mitigating child sexual exploitation and abuse material and activity. This included questions to some providers about the age assurance or verification they had in place to ensure the safe use of their services by children and enforce any age policies.

[1027] Online Safety (Basic Online Safety Expectations) Determination 2022 (Determination), section 13.
[1028] Online Safety (Basic Online Safety Expectations) Determination 2022 (Determination), sections 14 and 15.
[1029] Online Safety Bill 2021 – Explanatory Memorandum.

eSafety received responses from all these providers and published a report summarising the key information on 15 December 2022.[1030] The report found a significant variation in the steps being taken by providers to protect users and the wider Australian public.

With respect to age assurance measures, Omegle noted the age verification is difficult to enforce within linking to some other form of system (such as a bank account) or requesting a form of identification, which it commented raises issues including useability and privacy. Snap added that it considers age assurance can be disproportionately intrusive and against what it described as its core privacy-protecting principles on minimising the type of data it collects. Snap noted that age verification often requires access to, collection and retention of identity documents and expressed a view that it may introduce bias and inaccuracy where techniques rely on profiling or AI facial analysis.

In February 2023, reporting notices were issued to Google, Twitter, Twitch, TikTok, and Discord, similarly requesting responses to questions in relation to measures to address child sexual exploitation and abuse, as well as sexual extortion and the safe use of recommender systems. As with the first round of notices, these notices included questions to some providers about age assurance or verification. As of 30 June 2023, this regulatory process is ongoing, and eSafety will publish appropriate information once it concludes.

Future implementation of the Expectations

As set out in our regulatory guidance to the Expectations[1031], eSafety is planning a phased expansion of the reporting powers, starting with a focus on the acute harms from child sexual exploitation and abuse and shedding light on current practices in this area. We then intend to scrutinise industry practices in relation to other areas and start to track key safety metrics over time through periodic notices. We intend that reporting requirements will continue to cover age assurance and verification measures in place to ensure safe use. They may also include the section 12 expectation to make sure technological or other measures are in place and effective at preventing access to class 2 material (such as pornography) by children and young people.

Providers should have commenced reviewing their systems, processes, and policies once the Determination commenced to ensure compliance with the Expectations. They do not have to wait for government to mandate use of specific technologies (some of the steps currently being taken by industry are outlined in chapters 8 and 11). In relation to pornography, the reasonable steps will differ by service, depending on the user base, functionality, and policies. As noted in

[1030] eSafety Commissioner, '*Responses to transparency notices*', eSafety website, 2022, available at: https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices.

[1031] eSafety Commissioner, '*Basic Online Safety Expectations: Regulatory Guidance*', eSafety website, 2022, available at: https://www.esafety.gov.au/sites/default/files/2022-07/Basic Online Safety Expectations regulatory guidance.pdf.

chapter 6, eSafety considers that the measures taken by industry may differ depending on whether a service is dedicated to pornography, allows pornography, or prohibits it.

eSafety has committed to giving further guidance where necessary to support providers in determining the reasonable steps to implement the Expectations. Services can and should also consider this report in determining what steps may be reasonable to take.

eSafety will continue to improve transparency and accountability through its powers under the Act in relation to the Expectations. 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 verification pilot or mandate.

eSafety will also advise the Minister on if or how the Determination and the Act could be strengthened. Of note, eSafety cannot require reporting from some key parts of the online ecosystem, such as search services and app stores. This limits eSafety's and the public's understanding of the steps being taken to ensure safe use and prevent children from accessing harmful content.

Conclusion

There are multiple areas of the Act which enable eSafety to mitigate the harms posed by online pornography to children. They include functions for:

- research, education and cross-government coordination relating to online safety
- operationalising and enforcing the current regulatory frameworks applicable to online pornography, including the RAS Declaration, the Online Content Scheme, the industry codes and/or industry standards, and the Basic Online Safety Expectations.

In particular, the second phase of industry codes or standards development will provide an opportunity for enforceable measures across eight sections of the online industry to be introduced to help ensure relevant companies are doing their part to prevent and mitigate the harms associated with children's access to online pornography. The Basic Online Safety Expectations can work in complement to these codes or standards, providing an opportunity for enhanced transparency so eSafety and others can determine whether services are taking reasonable steps to keep children safe.

The government's ongoing classification review and the upcoming independent review of the Act will also provide opportunities to consider some of the issues stakeholders raised in eSafety's consultations. This includes, for example:

- the scope of services and content covered by the RAS Declaration, the Basic Online Safety Expectations, and/or the industry codes or standards
- the application of the classification framework to online pornography
- the application of the Act to emerging technologies that may change the way online pornography is created, access, or consumed, such as immersive technologies and generative AI
- the options available to eSafety to enforce any mandatory age assurance and complementary measures to prevent and mitigate harm to children from online pornography.
- eSafety notes that the introduction and enforcement of such measures will need to be supported by an appropriate level of resourcing.

eSafety next steps and recommendations for the Australian Government

eSafety next steps

Education

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.
- 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.

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.

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.

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

- 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.
- 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 complementary measures outlined in chapters 11 and 12 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 will hold further consultation when developing:

- Phase 2 industry codes or standards
- eSafety's input to the review of the Online Safety Act.

Recommendations for the Australian Government

Fund eSafety to:

- Review existing resources for alignment with the findings of the roadmap and background report.
- 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.

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.

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

- 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.

- 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.
  - 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.
  - 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.