



Australian Government

Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

Government response to the Roadmap for Age Verification

August 2023

Introduction

This is the Australian Government's response to the Roadmap for Age Verification (the Roadmap), which was developed by the eSafety Commissioner (eSafety) and delivered to Government on 31 March 2023.

The Roadmap acquits a key recommendation in the February 2020 House of Representatives Standing Committee on Social Policy and Legal Affairs (the Committee) report, *Protecting the Age of Innocence* (the report), which 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. The Government response to the report, released in June 2021, supported the recommendation and noted that the Roadmap would 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 makes a number of recommendations for Government, reflecting the multifaceted response needed to address the harms associated with Australian children accessing pornography.

This Government response addresses these recommendations, sets out the Government's response to this issue more broadly and outlines where work is already underway. This includes work being undertaken by eSafety under the *Online Safety Act 2021*, noting that since the Roadmap was first recommended in February 2020, the Australian Government has delivered major regulatory reform to our online safety framework with the passage of the Online Safety Bill on 23 July 2021 with bipartisan support, and the commencement of the Online Safety Act on 23 January 2022.

The Online Safety Act sets out a world-leading framework comprising complaints-based schemes to respond to individual pieces of content, mechanisms to require increased transparency around industry's efforts to support user safety, and mandatory and enforceable industry codes to establish a baseline for what the digital industry needs to do to address restricted and seriously harmful content and activity, including online pornography.

The Roadmap highlights concerning evidence about children’s widespread access to online pornography

Pornography is legal in Australia and is regulated under the Online Safety Act. Research shows that most Australian adults have accessed online pornography, with a 2020 survey by the CSIRO finding that 60 per cent of adults had viewed pornography.

However, pornography is harmful to children who are not equipped to understand its contents and context, and they should be protected from exposure to it online. Concerningly, a 2017 survey by the Australian Institute of Family Studies found that 44 per cent of children between the ages of 9-16 were exposed to sexual images within the previous month.

The Roadmap highlights findings from eSafety’s research with 16-18-year-olds, revealing that of those who had seen online pornography (75% of participants), almost half had first encountered it when they were 13, 14, or 15 years old. Places where they encountered this content varied from pornography websites (70%), social media feeds (35%), ads on social media (28%), social media messages (22%), group chats (17%), and social media private group/pages (17%). The Roadmap acknowledges that pornography is readily available through websites hosted offshore and also through a wide range of digital platforms accessed by children.

The Roadmap finds an association between mainstream pornography and attitudes and behaviours which can contribute to gender-based violence. It identifies further potential harms including connections between online pornography and harmful sexual behaviours, and risky or unsafe sexual behaviours.

The Roadmap finds age assurance technologies are immature, and present privacy, security, implementation and enforcement risks

‘Age verification’ describes measures which could determine a person’s age to a high level of accuracy, such as by using official government identity documents. However, the Roadmap examines the use of broader ‘age assurance’ technologies which include measures that perform ‘age estimation’ functions. The Roadmap notes action already underway by industry to introduce and improve age assurance and finds that the market for age assurance products is immature, but developing.

It is clear from the Roadmap that at present, each type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues.

For age assurance to be effective, it must:

- work reliably without circumvention;
- be comprehensively implemented, including where pornography is hosted outside of Australia’s jurisdiction; and
- balance privacy and security, without introducing risks to the personal information of adults who choose to access legal pornography.

Age assurance technologies cannot yet meet all these requirements. While industry is taking steps to further develop these technologies, the Roadmap finds that the age assurance market is, at this time, immature.

The Roadmap makes clear that a decision to mandate age assurance is not ready to be taken.

Without the technology to support mandatory age verification being available in the near term, the Government will require industry to do more and will hold them to account. The Australian Government has always made clear that industry holds primary responsibility for the safety of Australian users on their services. It is unacceptable for services used by children to lack appropriate safeguards to keep them safe. While many platforms are taking active steps to protect children, including through the adoption of age assurance mechanisms, more can and should be done. The Government is committed to ensuring industry delivers on its responsibility of keeping Australians, particularly children, safe on their platforms.

Government will require new industry codes to protect children

The effective implementation of the Online Safety Act is a priority of the Albanese Government, including the creation of new and strengthened industry codes to keep Australians safe online. The industry codes outline steps the online industry must take to limit access or exposure to, and distribution and storage of certain types of harmful online content. The eSafety Commissioner can move to an enforceable industry standard if the codes developed by industry do not provide appropriate community safeguards.

The codes are being developed in two phases, the first phase addressing ‘class 1’ content, which is content that would likely be refused classification in Australia and includes terrorism and child sexual exploitation material. The second phase of the industry codes will address ‘class 2’ content, which is content that is legal but not appropriate for children, such as pornography.

The codes and standards can apply to eight key sections of the online industry, which are set out in the Online Safety Act:

- social media services (e.g. Facebook, Instagram and TikTok);
- relevant electronic services (e.g. services used for messaging, email, video communications, and online gaming services, including Gmail and WhatsApp);
- designated internet services (e.g. websites and end-user online storage and sharing services including Dropbox and Google Drive);
- internet search engine services (e.g. Google Search and Microsoft Bing);
- app distribution services used to download apps (e.g. Apple IOS and Google Play stores);
- hosting services (e.g. Amazon Web Services and NetDC);
- internet carriage services (e.g. Telstra, iiNet, Optus, TPG Telecom and Aussie Broadband); and
- manufacturers and suppliers of any equipment that connects to the internet, and those who maintain and install it (e.g. of modems, smart televisions, phones, tablets, smart home devices, e-readers etc).

Phase 1

Work on the first phase of codes commenced in early 2022, and on 11 April 2022 eSafety issued notices formally requesting the development of industry codes to address class 1 material. On 1 June 2023, the eSafety Commissioner agreed to register five of the eight codes that were drafted by industry. The eSafety Commissioner assessed these codes and found that they provide appropriate community safeguards in relation to creating and maintaining a safe online environment for end-users, empowering people to manage access and exposure to class 1 material and strengthen transparency of and accountability for class 1 material.

The steps that industry must take under these codes include, for example:

- requirement for providers under the Social Media Services Code, including Meta, TikTok and Twitter, to remove child sexual exploitation material and pro-terror material within 24 hours of it being identified and take enforcement action against those distributing such material, including terminating accounts and preventing the creation of further accounts; and
- requirement for providers under the Internet Carriage Service Providers Code, including Telstra, iiNet and Optus, to ensure Australian end-users are advised on how to limit access to class 1 material by providing easily accessible information available on filtering products, including through the Family Friendly Filter program, at or close to the time of sale.

These registered codes will become enforceable by eSafety when they come into effect on 16 December 2023.

The eSafety Commissioner requested that industry revise the code for Search Engine Services, to ensure it accounts for recent developments in the adoption of generative AI, and made the decision not to register the Relevant Electronic Services Code and Designated Internet Services Code. The eSafety Commissioner found that these two codes failed to provide appropriate community safeguards in relation to matters that are of substantial relevance to the community. For these sections of industry, eSafety will now move to develop mandatory and enforceable industry standards.

The registered codes, including all of the steps industry are now required to take, are available at eSafety's website: www.esafety.gov.au/industry/codes/register-online-industry-codes-standards.

Phase 2

The next phase of the industry codes process will address 'class 2' content, which is content that is legal, but not appropriate for children, such as pornography.

In terms of the content of the code – which will be subject to a code development process – Section 138(3) of the *Online Safety Act 2021* outlines examples of matters that may be dealt with by industry codes and industry standards, and includes:

- procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult;
- procedures directed towards the achievement of the objective of ensuring that customers have the option of subscribing to a filtered internet carriage service;
- giving end-users information about the availability, use and appropriate application of online content filtering software;
- providing end-users with access to technological solutions to help them limit access to class 1 material and class 2 material;
- providing end-users with advice on how to limit access to class 1 material and class 2 material;
- action to be taken to assist in the development and implementation of online content filtering technologies; and
- giving parents and responsible adults information about how to supervise and control children's access to material.

In light of the importance of this work, the Minister for Communications has written to the eSafety Commissioner asking that work on the second tranche of codes commence as soon as practicable, following the completion of the first tranche of codes.

The Government notes the Roadmap recommends a pilot of age assurance technologies. Given the anticipated scope of the class 2 industry codes, this process will inform any future Government

decisions related to a pilot of age assurance technologies. The Government will await the outcomes of the class 2 industry codes process before deciding on a potential trial of age assurance technologies.

Government will lift industry transparency

The Government also notes that the *Online Safety Act 2021* sets out Basic Online Safety Expectations (BOSE) for the digital industry and empowers the eSafety Commissioner to require industry to report on what it is doing to address these expectations.

A core expectation, set out in section 46(1)(d) of the *Online Safety Act 2021*, is that providers ‘...will take reasonable steps to ensure that technological and other measures are in effect to prevent access by children to class 2 material provided on the service’. The *Online Safety (Basic Online Safety Expectations) Determination 2022* also provides examples of ‘reasonable steps’ that industry could take to meet this expectation, which includes ‘implementing age assurance mechanisms.’

The Commissioner is able to require online services to report on how they are meeting the BOSE. Noting the independence of the eSafety Commissioner’s regulatory decision-making processes, the Government would welcome the further use of these powers and the transparency that they bring to industry efforts to improve safety for Australians, and to measure the effectiveness of industry codes.

Government will ensure regulatory frameworks remain fit-for-purpose

The Government has committed to bring forward the independent statutory review of the Online Safety Act, which will be completed in this term of government. With the online environment constantly changing, an early review will ensure Australia’s legislative framework remains responsive to online harms and that the eSafety Commissioner can continue to keep Australians safe from harm.

The review of the *Privacy Act 1988* (Privacy Act Review) also considered children’s particular vulnerability to online harms, and the Privacy Act Review Report made several proposals to increase privacy protections for children online. The Government is developing the response to the Report, which will set out the pathway for reforms.

The Privacy Act Review Report proposes enshrining a principle that recognises the best interests of the child and recommends the introduction of a Children’s Online Privacy Code modelled on the United Kingdom’s Age Appropriate Design Code. It is recommended that a Children’s Online Privacy Code apply to online services that are likely to be accessed by children. The requirements of the code would assist entities by clarifying the principles-based requirements of the Privacy Act in more prescriptive terms and provide guidance on how the best interests of the child should be upheld in the design of online services. For example, assessing a child’s capacity to consent, 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.

The requirements of the Code could also address whether entities need to take reasonable steps to establish an individual’s age with a level of certainty that is appropriate to the risks, for example by implementing age assurance mechanisms.

More support and resources for families

While the Government and our online safety regulator will continue working with industry on this challenge, tools are already available to prevent children accessing pornography online.

The Government supports the eSafety Commissioner's work in developing practical advice for parents, carers, educators and the community about safety technologies. These products include online resources such as fact sheets, advice and referral information, and regular interactive webinars. These resources are freely available through the eSafety Commissioner's website at: www.eSafety.gov.au.

The Roadmap proposes the establishment of an Online Safety Tech Centre to support parents, carers and others to understand and apply safety technologies that work best for them. The Government has sought further advice from the eSafety Commissioner about this proposal to inform further consideration.

The Roadmap also recommends that the Government:

- fund eSafety to develop new, evidence-based resources about online pornography for educators, parents and children; and
- develop industry guidance products and further work to identify barriers to the uptake of safety technologies such as internet filters and parental controls.

The Government supports these recommendations. In the 2023-24 Budget the Government provided eSafety with an additional \$132.1 million over four years to improve online safety, increasing base funding from \$10.3 million to \$42.5 million per year. This ongoing and indexed funding provides Australia's online safety regulator with funding certainty, allowing long term operational planning, more resourcing for its regulatory processes, and to increase education and outreach.

The eSafety Commissioner works closely with Communications Alliance – an industry body representing the communications sector – to provide the Family Friendly Filter program. Under this program, internet filtering products undergo rigorous independent testing for effectiveness, ease of use, configurability and availability of support prior to certification as a Family Friendly Filter. Filter providers must also agree to update their products as required by eSafety, for example where eSafety determines, following a complaint, that a specified site is prohibited under Australian law.

Communications Alliance maintains a list and access details of certified filters at: www.commsalliance.com.au/Activities/ispi/fff.

Addressing the harms that can result from children's exposure to pornography

The Roadmap notes that age-appropriate, inclusive, evidence-based, and stigma-free education about online safety, sexuality, consent, and respectful relationships are integral to addressing the harms associated with online pornography.

The Roadmap recommends development of a mechanism for greater national coordination and collaboration of respectful relationship education. The Australian Government supports this recommendation. Through the Consent and Respectful Relationships Education (CRRE) commitment of \$83.5 million over 6 years (2022-23 to 2027-28), the Australian Government is working with states, territories, the non-government school sector and experts through a National Respectful Relationships Education Expert Working Group (Expert Group) to support the delivery of age-

appropriate, evidence-based, and expert-developed respectful relationships education, aligned to the Australian Curriculum. The Expert Group will also provide guidance on a rapid review on the delivery of CRRE, identifying gaps and opportunities, and also support the development of a national framework to guide schools in delivering high quality CRRE.

The Government is also committed to coordination and collaboration through the *National Plan to End Violence against Women and Children 2022-2032* (the National Plan). The National Plan acknowledges that the relationship between viewing pornographic content and violence is complicated. It notes that pornographic content that showcases violence and a lack of consent, could be linked to a young person's attitudes and beliefs about sex, intimacy, consent, and gender-roles in relationships. The Commonwealth and all states and territories - along with victim-survivors, experts, frontline services and other stakeholders – have contributed to the National Plan, which provides the blueprint to end gender-based violence in a generation.

Initiatives under the National Plan

In its last two Budgets, the Australian Government has made a \$2.3 billion investment in women's safety including to support implementation of the National Plan. This includes committing \$39.9 million to develop a new national prevention campaign on consent and respectful relationships. The consent campaign aims to prevent sexual violence by supporting adults with influence on young people to help them to develop positive attitudes and behaviours around consent. The first phase is expected to encourage adults to have conversations on consent and healthy relationships with each other, followed by sharing this understanding with young people (phase 2). This campaign is under development and is subject to Government approvals.

The Government also committed \$3.5 million under the National Plan to support Teach Us Consent to curate, develop and distribute social media resources on consent for young people aged 16 and over, and develop a youth advisory group. The program is expected to improve the attitudes and understanding of young people about consent, their capacity to have conversations about consent, and ultimately, to reduce sexual violence. The youth-led expert advisory group is expected to provide advice about what works when engaging young people on consent and sexual violence prevention.

Further, the 2022-23 Budget included \$100.4 million over 5 years (GST exclusive) to continue supporting Our Watch to deliver on key priorities of the National Plan, and continue existing successful initiatives for the primary prevention of violence against women and children. Through the Primary Prevention Activities program, Our Watch is funded to deliver *The Line* - a primary prevention social marketing campaign, designed to encourage adolescents and young adults aged 14 plus years to engage with age appropriate and evidence based information that educates on: [consent](#); [dating](#); [respectful relationships](#); [masculinity](#); [sex](#); [emotions](#); and [pornography](#). *The Line* also provides resources for [Educators and practitioners](#) and [parents and carers](#).

In addition, under the National Plan, the Government has funded eSafety:

- \$10.0 million for the Preventing Tech-Based Abuse of Women Grants Program to develop primary prevention initiatives that address the drivers of technology-facilitated gender-based violence;
- \$16.6 million to develop a Technology-Facilitated Abuse Support Service for victim-survivors and their frontline service staff;
- to deliver training and capacity building of frontline workers and other key cohorts to recognise and respond to technology-facilitated family, domestic and sexual violence;

- to deliver the eSafety Kids and TFA Program to raise awareness about how technology-facilitated abuse affects young people; and
- to work in formal partnership with Aboriginal and Torres Strait Islander peoples to ensure policies and services are culturally competent, strengths-based and trauma informed and meet the needs of Aboriginal and Torres Strait Islander peoples and communities.

Investing in research and building the evidence base

The Roadmap notes that the evidence around the potential impacts of online pornography on children is complex and conflicting, and recommends that the Government conduct new and specialist research in this area. This includes looking at the attitudes towards and impacts of online pornography on at-risk groups, particularly those who are underrepresented in the existing literature.

The Government supports this recommendation. Australia's National Research Organisation for Women's Safety (ANROWS) was established as an initiative of Australia's first *National Plan to Reduce Violence Against Women and their Children 2010-2022*, and their primary function is to build the evidence base that supports ending violence against women and children in Australia. The October 2022-23 Women's Safety Budget confirmed funding of \$23.3 million over 5 years from 2022-23 for the ANROWS National Priority Research Fund. ANROWS has identified three research streams for the National Priority Research Fund: perpetration, Aboriginal and Torres Strait Islander people, and Sexual Violence in Australia. This additional funding will:

- increase understanding of and responses to address the unique, intersecting and lifelong impacts of violence against certain communities, including Aboriginal and Torres Strait Islander peoples and the LGBTIQ+ community;
- build knowledge and understanding of the factors correlated with men perpetrating violence, including the role of their own lived experience of violence and trauma;
- recognise and address the patterns of behaviour that constitute coercive control, including through increased understandings of non-physical forms of violence and abuse, such as psychological abuse, technology-facilitated and financial abuse; and
- bring sexual violence out of the shadows by recognising barriers to reporting and acknowledging sexual violence as a standalone issue that occurs beyond intimate partner violence.

Working with counterparts

As technology advances, age assurance or verification processes that could be effectively implemented while preserving Australians' privacy and security, may emerge. The Roadmap describes how some online services are now trialing or introducing age assurance measures. A number of overseas governments, including of France, Germany, the UK, Utah and Louisiana, are considering or implementing age assurance requirements, and intergovernmental collaborative networks and accreditation frameworks are being developed.

In particular, the UK is a key likeminded partner in which Australia is continuing to deepen its engagement with across a range of strategic online safety and security matters. Both Australia and the UK are well-placed to shape and promote harmonious and globally-applicable principles and approaches in regards to age assurance technologies, age-appropriate design, and safety by design principles and practices.

The Government will continue to monitor the implementation and effectiveness of global and industry developments to inform our efforts in the future, and it is anticipated they will be

considered as part of the statutory review of the Online Safety Act, which is expected to commence in 2024.

Conclusion

The first duty of any Government is to protect its citizens from harm – a duty that also applies to the online world. In the modern digital environment where children are growing up with close access to technology, protecting them from exposure to online pornography is a complex task. Protections must be proportionate to the level of harm and respect the rights of citizens to privacy and security. Protections must also be effective and enforceable.

Australia has a strong track record in measured, targeted action in response to online harms which has included the establishment of the world's first eSafety Commissioner and legislating dedicated schemes to protect Australians from a range of online harms. The Australian Government is focused on the ongoing work needed to successfully implement the Online Safety Act, in particular the much needed 'step up' by the digital industry to protect Australian children from exposure to online pornography. The Government will continue to monitor these efforts closely.

The Government also takes seriously the need to address the drivers of gender-based and sexual violence. Under the National Plan, we are working with all state and territory governments, businesses and workplaces, media, schools and educational institutions, the family, domestic and sexual violence sector, communities and individuals, to achieve the shared vision of ending gender-based violence in one generation.

The Government thanks the eSafety Commissioner and all those who have contributed to the Roadmap for Age Verification.