Australian Government

Australian Government response to the House of Representatives Select Committee on Social Media and Online Safety report

March 2023

Contents

Establishment of the Inquiry

This is the Australian Government's Response to the Final Report of the House Select Committee on Social Media and Online Safety (the Committee), which was presented on 15 March 2022.

The Government notes that this Committee was established on 1 December 2021 in the final sitting week of 2021 towards the end of the final term of the Morrison Government.

The Inquiry was established to consider a range of matters related to online safety and the actions of digital industry in Australia, yet commenced before the *Online Safety Act 2021*, which empowered the eSafety Commissioner with a range of new powers to support online safety, came into effect on 23 January 2022. The Inquiry had broad-ranging terms of reference but was required to report in only 4 months and to hold the bulk of its hearings over the summer period. While the Committee provided its report to Government in March 2022, the former Government did not respond before the Parliament was prorogued.

The Albanese Government takes its commitment to protect Australians from all forms of online harms seriously. We understand the importance of listening and responding to Australians who are impacted by online harms, particularly those who are most vulnerable. We have taken the time to consult widely across the Australian Government on our response to the Final Report to ensure it provides a comprehensive view of the work underway in relation to the matters considered by the Committee.

This response provides detail on work underway across a number of portfolios, including Communications, Home Affairs, Attorney-General's and Social Services, and work being led by Australia's independent online safety regulator, the eSafety Commissioner.

We appreciate the work of the Committee and would like to thank everyone who contributed to the Inquiry into Social Media and Online Safety.

Australian Government response

The Government's online safety agenda

The safety of Australians is a core priority of the Albanese Government, including online. It is fundamental that our online world, which is so much a part of our daily lives, provides safe and inclusive environments, maximises the benefits of the digital economy and supports social cohesion.

These goals require a holistic, multi-faceted approach, including a robust legislative framework, strong regulators which can hold platforms to account, technological measures to prevent harms, and a population with high levels of digital and media literacy.

Australia has a strong track record in online safety. The *Online Safety Act 2021*, and the mechanisms in the preceding *Enhancing Online Safety Act 2015* and *Broadcasting Services Act 1992* set out a novel system for the removal of harmful content online and the provision of education, support and advice to help Australians stay safe online and get help when things go wrong.

But the online world is continually changing and Australia's approach needs to evolve. The Albanese Government is pursuing three immediate priorities.

First, is the **effective implementation and ongoing review of the Online Safety Act.**

The Albanese Government remains committed to the coordinated and systematic implementation of the Online Safety Act (the Act). This regulation received bipartisan support in the parliament, and the Albanese Government is now working with the eSafety Commissioner to undertake the critical work to implement the Act following its commencement in January 2022. The Government is also focused on driving awareness of eSafety so Australians can access and make the most of eSafety's resources.

While the Act has a wide scope, and plays an important role in promoting safe online environments, it does not address all risks, and there remain a number of gaps in the broader online safety equation in Australia.

Our second priority is **tackling gaps in the current framework**. There is a need for additional and complementary policy levers that will enable us to be responsive to emerging risks and opportunities as technology advances and as consumer preferences change. In recognition of this, we are taking action across a range of workstreams to address these gaps. This work is being led by a number of portfolios across the Government.

Our third priority is supporting **cross-government coordination on the regulation of online harms**.

We recognise that to deliver on our overarching goal of providing safe and inclusive online environments that maximise the benefits of the digital economy and support social cohesion, we must be coordinated in our efforts. The Albanese Government is committed to ensuring the regulation of online harms is coordinated, and that engagement between community, industry and civil society stakeholders and the Government is streamlined.

This document details work underway to deliver on each of these priorities and provides the Government's response to the specific recommendations made by the Committee.

1. Implementation of the Online Safety Act

The Online Safety Act (the 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 a set of industry codes to establish a baseline for what the digital industry need to do to address illegal and seriously harmful content and activity facilitated by their services.

The ongoing implementation of the Act is a key priority for the Government and the eSafety Commissioner. In December 2022, the eSafety Commissioner published a summary of industry's responses to the first set of reporting notices issued under the Basic Online Safety Expectations (BOSE), which related to child sexual exploitation and abuse material. A second round of notices were issued in February 2023 and further notices will be issued over coming months, with the focus areas informed by the criteria set out in the Act. In addition, the eSafety Commissioner will shortly make a decision on whether to register industry codes aimed at addressing the most seriously harmful online content.

The eSafety Commissioner also continues its vital education and awareness-raising activities, working closely with the education sector, law enforcement, civil society and the broader community to build awareness around online safety. This includes supporting children and their teachers, parents and carers to navigate the online world safely; raising awareness of resources eSafety has developed to support vulnerable groups; and strengthening referral pathways so that regardless of where someone goes when they experience online harm, they receive the support they need.

An independent review of the Act must commence by January 2025 and is to consider whether any amendments to the Act or the rules are required. Recognising that the online world is evolving quickly, the Albanese Government commits to undertake and complete this review earlier than required and within this term of Government so that Australia and our world-leading online safety framework remain fit for the changing online environment.

2. Tackling gaps in the current framework

Over the coming months, the Australian Government will take immediate action on a range of online harms that are not adequately captured under existing regulatory frameworks, as well as deliver on a key election commitment to make digital and media literacy products developed by the Alannah & Madeline Foundation freely available to all schools in Australia. Those harms with work underway include: online hate speech, mis- and disinformation, scams, gambling-like content in online games, and online dating safety.

The Attorney-General has launched a national consultation on the Privacy Act Review and will take forward critical work which stagnated under the former government to ensure Australia's privacy framework is fit for the digital world.

In March 2023, the Government will receive the Age Verification Roadmap developed by eSafety in response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report, 'Protecting the age of innocence', which asked eSafety to consider if, and how, a mandatory age verification mechanism could practically be achieved in Australia. A response to the Roadmap is expected later in 2023.

Digital and media literacy

Digital literacy – the ability to use technology and understand how digital environments work – and media literacy – the ability to critically engage with media of all types in all aspects of life – are critical for equipping Australians to have positive experiences in online settings. Media literacy can also

improve social cohesion; increase civic engagement; and empower individuals to be positive agents for cultural change. It is important that individuals have the skills and competencies to curate their own experience of the digital world and to self-mediate their exposure to a myriad of influences online. Equally, industry must facilitate and encourage the development of these skills by providing tools and information for users.

In the 2022-23 October Budget, the Government committed $6 million over three years for the national rollout of the eSmart Digital Licence+, eSmart Junior Digital Licence+ and eSmart Media Literacy Lab. These eLearning tools, developed and delivered by the Alannah & Madeline Foundation, will be freely available to all schools in Australia, not just those that can afford them. The tools will help Australian students develop the skills they need to be critical, safe, responsible and active citizens online.

Media literacy is a lifelong process. The Government recognises we need to better understand the state of media literacy levels in Australia, who in our society will need additional support and what that support will look like. Work is underway across Commonwealth departments and agencies to align objectives, principles and priority focus areas linked to media literacy.

Online hate speech

All people are entitled to respect, equality, dignity, and to be free from hatred or harassment, including in the online world. Hatred and hate speech can dehumanise and denigrate particular groups, create division in the community and undermine Australian values such as social cohesion, freedom of expression and inclusiveness. In the online environment, it can spread faster and further than in an offline environment, magnifying its impacts.

The online world has also seen the emergence of new forms of hate and the re-emergence of others, including Holocaust denial, extreme misogyny and racist hate speech. Some communities disproportionately experience online hate speech, including First Nations people, people from culturally and linguistically diverse backgrounds, religious groups, the LGBTQI+ community and people with disability.

While the Online Safety Act includes some mechanisms to address more extreme forms of hate speech (for example, instances of hateful or dehumanising commentary where it meets the definition of 'adult cyber abuse'; and against material that incites violence or promotes crime or terrorism), it does not confer specific powers on the eSafety Commissioner in relation to online hate or vilification, particularly that which targets groups and communities. Action to address this harm is long overdue.

The Government is considering what more can be done to address group hate speech online. We will take a principled and evidence-based approach to ensure the response is effective and supports members of our community who are targeted by online hate.

Misinformation and disinformation

The Government is committed to protecting Australians and our democratic values from the harmful spread of dis- and misinformation online. Dis- and misinformation, while not regulated by the Online Safety Act, forms a significant component of the broader online safety environment, and their rapid spread via digital platforms has become a significant problem. They erode trust in democratic institutions, undermine public health efforts, contribute to social division, and can be a vector of foreign interference.

In June 2021, the Australian Communications and Media Authority (ACMA) delivered a report to the former Government – *A report to government on the adequacy of digital platforms' disinformation and news quality measures*. In response, the Government has announced plans to give the ACMA new

information gathering, record keeping, and reserve code registration and standard making powers to strengthen the current voluntary industry framework to combat online dis- and misinformation.

These powers are intended to ensure transparency in the implementation of measures by platforms to combat dis- and misinformation; provide increased visibility of systemic issues; incentivise platforms to act; and, if platform actions prove insufficient, provide Government with avenues for intervention by registering industry codes or making a standard. The powers will focus on systemic issues, not individual pieces of content, and are intended to complement the existing voluntary industry code.

Consultation on the Exposure Draft of the Bill for these powers will occur in the first half of 2023, with legislation to be introduced by the end of the year.

Online scams

Every year, scams cost Australians, businesses and the economy billions of dollars and cause untold emotional harm and mental stress to victims and their families.

In its 2022 Targeting Scams report, the Australian Competition and Consumer Commission (ACCC) stated that nearly $1.8 billion in losses were reported to Scamwatch, ReportCyber, various financial organisations and other government agencies in 2021. Taking into consideration that around 30 per cent of scam victims don't report, the estimated real loss is well over $2 billion. In addition, the percentage of online scams is growing faster than any other medium. Financial losses reported to Scamwatch from scams conducted via social networking and mobile apps almost doubled between 2020 ($49 million) and 2021 ($92 million). However, the cost of scams is far more than just financial – scams also lead to emotional stress and can have life changing consequences for many individuals, families, and businesses. Older and more vulnerable Australians have been particularly preyed upon.

The Government is committed to a new long-term, coordinated, whole-of-government approach to reduce Australians' losses to scams. This includes through strengthening industry codes to clearly define the private sector's responsibilities for protecting consumers from scams, with the involvement of industry members including banks, telecommunications providers and digital platforms; and through the phased establishment of a National Anti-Scams Centre.

Consultation is also underway on a response to the ACCC's fifth interim Digital Platforms Services Inquiry report, which will inform further Government action to address scams with regard to digital platforms.

Gambling-like content in online games

The Government appreciates that there is strong community concern about gambling-like content such as 'loot boxes' and 'simulated gambling' in online games, particularly those played by children and young people, due to similarities with real-world gambling and an increasing body of evidence linking use of these games with a range of harms, including problem gambling.

The Government is consulting with state and territory governments to introduce minimum classification ratings of M (Mature - not recommended for persons under 15 years) for games with loot boxes, and R 18+ (restricted to adults 18 and over) for games that feature simulated gambling. These proposed ratings will provide a stronger signal that such games may not be appropriate for children or minors.

This work responds to the growing body of evidence around harms associated with gambling-like features in games, and also takes forward recommendations made in the 2020 Review of Australian Classification Regulation (Stevens Review). This review was never released by the former Government, and the Albanese Government is now beginning the important work of updating Australia's outdated classification scheme to make it fit for the digital world.

Online dating safety

Research published by the Australian Institute of Criminology in October 2022 found that three-quarters of users were subjected to some form of online sexual violence, and one third of users were subjected to in-person sexual violence, perpetrated by someone they met on a dating app or website.

In January 2023, the Government convened the National Roundtable on Online Dating Safety, bringing together government; the online dating industry; the family, domestic and sexual violence sector; diversity and inclusion organisations; and researchers to consider what more can be done to prevent exploitation of dating apps to facilitate gender-based and sexual violence.

Roundtable participants agreed four areas of further work, including:

1. Preventing exploitation of online dating services by perpetrators;
2. Supporting users who experience harm;
3. Empowering users with information on safer online dating practices; and
4. Greater uptake of technological solutions to prevent harm.

The Government will provide an update on these outcomes by the end of March 2023.

Privacy Act Review

The Privacy Act Review Report, released by the Attorney-General in February 2023, puts forward a range of proposals designed to ensure Australia's privacy framework responds to new challenges in the digital era, better aligns with global standards of information privacy protection and properly protects Australians' privacy.

Of particular relevance to online safety, the Report includes proposals regarding consent and privacy default settings, targeted advertising and online content, and a Children's Online Privacy Code which would govern how social media and digital platforms use children's data.

Public consultation on the Report is currently underway.

3. Cross-government coordination on online harms

Successfully addressing online harms requires a cross-portfolio effort across the Australian Government. While responsibility for addressing online safety primarily falls in the Communications portfolio, there is complementary work underway in the Attorney-General's, Home Affairs, Treasury, Social Services, Education and Industry portfolios. This reflects the reality that many harms that occur online are extensions of harms that have long occurred in the offline world.

While there is clearly a need for significant policy action to address the substantial and evolving harms in this space, the committee heard evidence that a lack of process coordination undermined the effectiveness of regulation and created real costs.

The Albanese Government will take steps to ensure policy is coordinated across those portfolios with responsibility for regulating digital platforms and addressing online harms, as well as to streamline engagement for members of the public, industry and civil society, and ensure Government policy is informed by up to date research about online harms.

First, to complement the work of the Digital Platform Regulators Forum which was established in March 2022, the Government will hold a bi-annual meeting of Ministers with responsibility for addressing online harms to discuss cross-cutting issues and ensure a joined-up approach across Government. This will formally align policy objectives across Government to address online harms experienced by Australians and support consideration of what other reforms may be required in a proactive and coordinated way.

Second, the Government will refer matters of public interest on regulation of online harms and the digital industry to the House of Representatives Standing Committee on Communications and the Arts, to support engagement on these important issues from across the Parliament. Utilising the existing standing committee will support the continuation of the longstanding nonpartisan approach taken across Government and Opposition on online safety. The Government intends the committee will have a role in considering emerging trends, new technologies, research on online harms, and international approaches. The Government welcomes the involvement of supplementary members on inquiries that may be of interest to a broader range of Members of Parliament.

Conclusion

Online safety is a shared responsibility. This means that there is a role for industry, governments, parents, carers and kin, teachers, individual users and the broader community to promote and maintain online safety for Australians. While industry has primary responsibility for the safety of their users and the Government is committed to ensuring industry delivers on that responsibility, we are also committed to empowering Australians with the skills to navigate the online world safely and protect themselves online. We want to stop harms before they occur.

We look forward to working with Australians, industry and community organisations and are committed to hearing from diverse voices and those that have direct experience of online harms to inform our future policy development.

The remainder of this document sets out the Government's response to the specific recommendations made by the Committee.

The Government's response to recommendations of the Committee

Resourcing for the eSafety Commissioner, education, awareness and engagement with youth, and law enforcement

Funding eSafety

There are three recommendations in the Final Report which relate to eSafety funding, including: to review funding to ensure that the eSafety Commissioner is adequately and appropriately funded (**Recommendation 25**); to undertake research to better understand emerging issues, including how cultural change is achieved in online settings (**Recommendation 3**); and to provide additional funding for eSafety to establish and manage an online single point of entry reporting service for victims of online abuse (**Recommendation 6**).

The Government is committed to supporting the eSafety Commissioner's legislated responsibility to promote online safety for Australians, and ensuring that the functions and responsibilities of the office of the eSafety Commissioner are adequately and appropriately funded.

The Government is aware that the majority of eSafety's funding is non-ongoing or terminating, with annual funding forecast to decline after 2022-23, as a result of funding decisions taken by the former Government. The Government will review eSafety's ongoing funding in a future Budget.

The Government has developed specialist services, processes and legislative approaches in response to the different online harm types.

- The eSafety Commissioner plays a central role for Australians to report cyberbullying of children, adult cyber abuse, image-based abuse and illegal and restricted content (such as child sexual abuse material) through its complaints-based schemes.

- Reports of online child sexual abuse made to eSafety must be referred to the Australian Federal Police (AFP)-led Australian Centre to Counter Child Exploitation (ACCCE) for effective triage, evaluation and referral for investigation.

- The ACCCE ensures appropriate and timely responses to reports of child sexual exploitation and abuse through 24/7 rostering and on-call arrangements with specialist investigators.

- In addition to reports to eSafety and the ACCCE, Australians are also able to report specific types of cybercrime through the ReportCyber portal (accessed at cyber.gov.au/report). ReportCyber is hosted by the Australian Signals Directorates' Australian Cyber Security Centre and provides an online platform to report identity theft, online fraud, cyber security incidents, ransomware and malware, and cyber abuse. Reports to ReportCyber are referred to the appropriate police jurisdiction for assessment.

To build the evidence base around online harms, the Government supports research to better understand online safety issues. There is a range of Government-funded research underway to understand online behaviours and change approaches online. The Government supports continuing research in this space which is undertaken by a number of agencies across Government, reflecting the broad scope of issues and cross-government responsibility for supporting cultural change. Agencies that undertake research in this space include eSafety, as well as the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA); the ACCCE; the Department of Social

Services (DSS); the Attorney-General's Department (AGD); the Australian Institute of Criminology; and the Department of Home Affairs. The Government commits to holistically consider this research to inform the approach to any future regulation.

Raising awareness of support and resources

There are two recommendations in the Final Report regarding education and awareness campaigns; including: a campaign focussing on digital citizenship, civics and respectful online interaction (**Recommendation 4**); and a campaign to raise awareness of the eSafety Commissioner's powers to remove harmful content and reporting mechanisms (**Recommendation 23**).

The Government recognises the importance of early intervention, education and awareness campaigns and programs in impacting cultural change. There are several existing educational and awareness campaigns which seek to reduce the prevalence of online harms by focussing on establishing positive behaviours, respectful online interaction and highlighting digital citizenship and civics, including:

- In the 2021–22 Budget the Australian Government committed $5.2 million for a **national online safety awareness campaign** (the Campaign) to improve awareness of the support and resources offered by the eSafety Commissioner under the Online Safety Act. The campaign had a particular focus on women, First Nations and culturally and linguistically diverse audiences, and people with disabilities through dedicated channels with bespoke materials. In the 2022–23 October Budget, the Australian Government committed an additional $5.0 million over five years (2022–23 to 2026–27) to extend the Campaign which is led by DITRDCA.

- The eSafety Commissioner's '***SCROLL' campaign***, which launched on 20 June 2022, features content on a range of online safety issues for young people, including on online consent and respectful relationships, finding one's community and ways to support friends that may be experiencing harm online.

- DSS's ***Stop it at the Start*** campaign aims to break the cycle of violence by encouraging adults to reflect on their attitudes and have conversations about respectful behaviours with young people aged 10 to 17. Four phases of the campaign have been delivered since it first launched in 2016. Additional funding was provided in the October 2022–23 Budget to deliver a fifth and sixth phase of the campaign, which will continue to drive positive change in behaviours and attitudes around violence against women and help to promote gender equality over time.

- Our Watch's **No Excuse for Abuse** campaign, funded by DSS, aims to raise awareness of non-physical abuse, including technological abuse. The campaign launched in 2020 and resources are available at the No Excuse for Abuse website: https://www.noexcuseforabuse.org.au/.

- The Australian Electoral Commission introduced the ***Stop and Consider*** campaign in the lead up to the 2019 federal election and again in the lead up to the 2022 federal election. The campaign aims to help voters 'Stop and Consider' the electoral communication they encounter, including whether it is from a reliable source, whether the information is current, and whether it may be a scam or is safe. This engagement is focussed solely on electoral communications and is only in the market in the lead up to a federal election.

The Australian Government also funds a range of relevant education programs, including: The Be Connected program which provides resources and online training modules for older Australians to help improve their digital literacy and confidence to engage safely online (run in partnership with eSafety, DSS and the Good Things Foundation); eSafety's Online Safety Community Grants Program; and the Department of Education-led Consent and Respectful Relationships Program.

Despite these investments, awareness of the Safety Commissioner is low. A 2022 National Online Safety Survey found that unprompted, only two per cent of parents surveyed identified the eSafety

Commissioner as an organisation they'd turn to for help with online safety. Clearly, not enough people are aware of the eSafety Commissioner and the important resources and support that eSafety can provide. Improving awareness of eSafety is a priority for the Government.

Online safety education

There are two recommendations in the Final Report that relate to online safety education, including: to increase the reach of educational programs for young people (**Recommendation 21**); and designing and implementing a national strategy on online safety education, including a proposed curriculum, for early childhood, primary and secondary school students (**Recommendation 22**).

The Government agrees that education is vitally important when it comes to enabling Australians to stay safe and thrive online. Work is now underway to provide education and resources to schools, children and young people, and families.

- In the 2022–23 October Budget, the Australian Government committed $6 million over three years (2023–24 to 2025–26) to support the national rollout of digital and media literacy eLearning tools developed and delivered by the Alannah & Madeline Foundation. Together, the eSmart Digital Licence+ for students aged 10 to 14, the eSmart Media Literacy Lab for secondary students aged 12 to 16, and a new eSmart Junior Digital Licence+ for primary students aged 5 to 9 will be made freely available to every Australian school. These products will help Australian students develop the skills they need to be critical, safe, responsible and active citizens online.

- The Australian Curriculum is developed by the Australian Curriculum, Assessment and Reporting Authority (ACARA), an independent statutory body. ACARA reviewed the curriculum between 2020-2022 and an updated version was endorsed by all Education Ministers on 1 April 2022 for implementation in schools from 2023. The Australian Government plays a leadership role in setting and advocating for national priorities in school education; state and territory governments and non-government school authorities have responsibility for managing schools, including implementation of the curriculum in line with system and jurisdictional policies and requirements. In consultation with the eSafety Commissioner, ACARA made significant changes to the Digital Technologies learning areas and the Digital Literacy general capability to ensure that students learn to use a variety of digital platforms safely. Likewise, the Online Safety Curriculum Connection was developed in consultation with the eSafety Commissioner and links to a number of components in the Australian Curriculum at all year levels. The eSafety Commissioner will continue to engage with ACARA to assist with curriculum development related to Digital Technologies and Health, and Physical Education. Themes and topics include online safety, mental health, and respectful relationships.

- A core function of the eSafety Commissioner is to support, encourage, conduct, accredit and evaluate educational programs relevant to online safety. Within this remit, the eSafety Commissioner has delivered a range of evidence-based resources to educate children and young people, their parents and carers on preventing and responding to online harms. The eSafety Commissioner has also developed a Best Practice Framework for Online Safety Education and a Toolkit for Schools to support a nationally consistent approach to online safety education.

- The eSafety Commissioner provides specific educational resources, accredited teacher professional learning, education for parents and carers, and training for other professionals working with children and young people. The eSafety Commissioner also works with external providers to increase access to high quality online safety education in schools. The Trusted eSafety Provider program endorses providers of online safety education whose programs align with the Best Practice Framework and who are required to provide information about eSafety's reporting mechanisms in each program they deliver.

- In December 2022, the eSafety Commissioner established the Online Safety Education Council to coordinate online safety education with 22 education authorities in states and territories to promote best practice and national consistency. The group will also raise awareness of reporting and support agencies, and provide opportunities for better coordination of responses to critical online safety issues.

- The eSafety Commissioner's online safety education efforts are complemented by the AFP-led ThinkUKnow Program. Through ThinkUKnow, the AFP delivers prevention, awareness and education initiatives (including in-school presentations) on online child sexual exploitation and abuse, including on online grooming.

Youth engagement

There is one recommendation in the Final Report focussing on the importance of youth engagement in considering online safety issues (**Recommendation 26**).

The Government agrees that direct and formal engagement with young people on online safety issues is essential.

To this end, the Government welcomes the establishment of the eSafety Youth Council, which is coordinated and managed by the eSafety Commissioner and includes 24 members aged 13 to 24 years. The Council is an important forum for Government to hear directly from young people on issues they experience online and ways of supporting them to have positive experiences online. The Council was appointed in April 2022 and met throughout 2022 to discuss online safety issues facing young people.

The Council will report to Government after its first 24-month term with any outcomes and actions identified by the Council, as well as provide a 12-month interim progress report.

Training for law enforcement

There is one recommendation in the Final Report which recommends that the Government work with the states and territories to ensure law enforcement agencies are appropriately trained on how to support victims of online harm (**Recommendation 24**).

Work to implement this recommendation is already underway.

Under the *National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030* (National Strategy), the Australian Government is working with state and territory governments to enhance law enforcement responses to child sexual abuse in all settings, including online, and to support and empower victims and survivors.

The Government is also investing in law enforcement training, awareness raising and collaboration to bolster the capacity of police across Australia to respond to online harms. The ACCCE, in conjunction with states and territories, delivers specialist training programs to state and territory law enforcement agencies aimed at: detecting child abuse material being downloaded from file sharing platforms; victim identification awareness; and child exploitation.

The Government has committed $4.1 million over four years from 2022–23 under the Womens Safety Package and the *National Plan to End Violence against Women and Children 2022–32* (National Plan) for AGD to develop and deliver a training package for police across Australia to enhance responses to family, domestic and sexual violence. Training will include a particular focus on technology-facilitated abuse, coercive control, sexual assault, child safety, and will target problematic attitudes and behaviours. As part of delivering the training package, AGD will work closely with eSafety to leverage existing programs, including the eSafety Women program, which deliver capacity-building training on technology-facilitated abuse to frontline workers.

eSafety has memoranda of understanding (MoU) with the AFP, including the ACCCE, as well as every state and territory police force. These are being updated to reflect eSafety's broader powers and functions under the Online Safety Act. These MoU arrangements provide for referral pathways from eSafety to law enforcement agencies when online activities reach the criminal threshold, as well as from law enforcement agencies to eSafety where it is best placed to provide support. eSafety also works collaboratively with the AFP and state and territory police forces to ensure their awareness of eSafety's reporting schemes and support available on eSafety's website. eSafety delivers customised online safety education sessions and resources to police forces and continues to work with law enforcement to uplift knowledge about eSafety issues.

Technology-facilitated abuse

There are two recommendations in the Final Report regarding technology-facilitated abuse; including to conduct an inquiry into technology facilitated abuse, including how it is regulated at law (**Recommendation 7**); and to significantly increase funding for specialised counselling and support services for victim-survivors of this form of abuse (**Recommendation 8**).

Family, domestic and sexual violence cannot be excused or justified under any circumstance. Ensuring the safety of all Australians is a priority of the Australian Government. The Government has committed to provide the focus and national leadership needed to deliver change.

The National Plan, delivered in October 2022, is the cornerstone of the Government's strategy to address family, domestic and sexual violence, including technology-facilitated abuse. It sets the national policy agenda for the next 10 years guiding the work of Commonwealth, state and territory governments, family safety experts and frontline services. The National Plan's vision is to end gender-based violence in one generation.

To realise this vision, the Government is investing a total $1.7 billion in funding towards implementing the National Plan and other women's safety initiatives. This investment is being made across the continuum of violence – from prevention and early intervention to response and recovery and healing.

The Government is mindful of the emotional toll placed on victim-survivors when asked to provide evidence at forums such as inquiries, and thanks those victim-survivors who shared their experiences with this Committee. The Government notes the existing evidence base on, and work underway to address, technology-facilitated abuse, including through the eSafety Women program and research undertaken by the Australian Institute of Criminology and Australia's National Research Organisation for Women's Safety.

The National Plan addresses the issues raised in recommendations 7 and 8. The National Plan recognises that technology-facilitated abuse is widespread and increasing, and can take many forms, including stalking, surveillance, tracking, threats, harassment, coercive control and the non-consensual sharing of intimate images. The focus on technology-facilitated abuse in the National Plan is supported by appropriate funding measures in the 2022–23 October Budget, including:

- $16.6 million over four years (2022–23 to 2025–26) for eSafety to develop a helpline service. This service will provide practical advice, support and guidance to victim-survivors of technology-facilitated abuse, and the frontline workers who support them, within the context of family, domestic and sexual violence.

- $57.9 million over five years (2022–23 to 2026–27) for DSS to continue the Keeping Women Safe in their Homes and the Safe Phones programs. Keeping Women Safe in their Homes supports victim-survivors to stay safe in their homes through risk assessments, safety planning, home security audits and case management. Safe Phones provides phones that have been

safely set up to avoid technology-facilitated abuse of women that have experienced family and domestic violence.

- Around $200 million over five years (2022–23 to 2026–27) to DSS for 1800RESPECT, the national domestic, family and sexual violence (including technology-facilitated abuse) counselling, information and support service which is available 24 hours a day, 7 days a week for anyone that has experienced violence, including technology-facilitated abuse.

In addition, Australia has a strong criminal offence and law enforcement framework to address technology-facilitated abuse. This includes a comprehensive set of computer and telecommunications offences under Parts 10.6 and 10.7 of the *Criminal Code Act 1995* (Cth), such as online child sexual exploitation and abuse (section 474.22), and cyber abuse including non-consensual sharing of intimate images (ss 474.17 and 474.17A).

The Government has also acted to address growing concerns about safety on dating apps, as a first step convening the National Roundtable on Online Dating Safety in January 2023. This roundtable brought together members of Commonwealth and state and territory governments and representatives from the online dating industry; the family, domestic and sexual violence sector; diversity and inclusion organisations; and research bodies to consider what more can be done to prevent exploitation of dating apps to facilitate gender-based and sexual violence. Further work is being undertaken in collaboration by DITRDCA, DSS, AGD, the Domestic, Family and Sexual Violence Commissioner, the eSafety Commissioner, the family, domestic and sexual violence sector and the dating app industry. Minister Rowland has agreed to provide an update on these outcomes by the end of March 2023.

Emerging harms and emerging solutions

Online abuse of public figures

There is one recommendation in the Final Report which focuses on the extent to which platforms apply different standards to victims of online abuse if they are a public figure (**Recommendation 12**).

The Government agrees that all Australians should be safe online, whether they are public figures or private citizens. Evidence heard by the Committee of examples of the online abuse experienced by public figures is concerning and does not align with the Government's priority that industry should enforce their terms of service consistently and transparently.

DITRDCA will provide advice to Government, in consultation with eSafety, on whether additional regulatory or non-regulatory options are required to address the concerns heard by the Committee around whether different standards apply to victims of abuse depending on whether they are a public figure.

Encryption

There is one recommendation in the Final Report which proposes that the Government should consider the need for regulation of end-to-end encryption (E2EE) technology in the context of harm prevention (**Recommendation 10**).

E2EE plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. Particular implementations of encryption technology, however, pose significant challenges to public safety and security. Digital industry's increasing adoption of anonymising technologies such as E2EE, are making online harms easier to commit without detection, facilitating and concealing serious national security related and criminal activity including online terrorism and violent extremism, child sexual abuse, identity theft, and drug and firearm trafficking.

The Australian Government does not advocate for weakening of E2EE. Instead, it advocates through international statements (such as the *International Statement: End-To-End Encryption and Public Safety* and inclusion in the 2021 Five Country Ministerial statement) to develop greater industry, government, and law enforcement collaboration to balance the three elements of strong and robust online trust – privacy, safety and security. Australia also continues to engage with international partners to call for digital industry to work with government to design their systems with user safety and protection in mind, and to align Australia's domestic efforts to counter online harms with emerging and maturing international norms.

Privacy, safety, security and lawful access are not mutually exclusive. It is possible to develop technology that protects the right to privacy, whilst also supporting law enforcement to keep the community safe. To mitigate the use of E2EE facilitating harm, the Department of Home Affairs, DITRDCA, eSafety, the Office of the Australian Information Commissioner (OAIC), and AGD will continue to work together to:

- gather evidence and analyse the impacts of E2EE on Australia's national security and public safety, including the impact of E2EE on online safety, particularly harms such as child sexual exploitation and abuse;
- explore whole of government policy positions and solutions to mitigate the risks posed by E2EE while maintaining privacy and security;
- support coordinated, comprehensive and constructive engagement with relevant digital industry, including encouraging industry to take a Safety by Design approach, and to invest in solutions that maintain safety, privacy, and security;
- examine the need for regulation of E2EE technology in the context of harm prevention, taking into account individual privacy and online security, and implications on public trust in these technologies;
- work with international counterparts to establish a unified and consistent approach to lawful access.

Algorithms

There are two recommendations in the Final Report which focus on the use of algorithms in digital platforms, including the types and scale of harms caused as a result of algorithm use (**Recommendation 13**); and the potential mechanism to require digital platforms to report on their use of algorithms (**Recommendation 14**).

The Government agrees that we need to better understand the operation of algorithms on digital platforms.

The Department of Home Affairs and DITRDCA are progressing work to understand the operation of algorithms on digital platforms. This work will also consider findings from other work underway across Government throughout 2023, including:

- AGD is progressing the development of a Government response to the report of the Privacy Act review, which included proposals to:
    - give individuals greater transparency over how entities use personal information to make automated decisions with a legal or similarly significant effect on individuals' rights is used and how such decisions are made, and how individuals are targeted with advertising and online content, including information about the use of algorithms and profiling to recommend content;

- give individuals more choice by requiring individuals' consent to their personal information being traded and allowing individuals to opt out of their personal information being used or disclosed for direct marketing and from receiving targeted advertising;
- prevent harmful targeting by requiring targeting to be fair and reasonable in the circumstances and prohibiting entities from targeting based on sensitive categories of information (with an exception for socially beneficial content);
- protect children by prohibiting trading in children's personal information and prohibiting direct marketing and targeting children unless it is in the child's best interests;

- The Digital Platform Regulators Forum's (DP-REG) literature review examining algorithms, focussing on algorithm use in recommender systems, content moderation and targeted advertising, to enhance members' understanding of associated regulatory risks; and
- The Department of Industry, Science and Resources' review into the regulation of artificial intelligence and automated decision making.

The Departments will jointly report back to Government by Quarter 1 2024 with options to build capability around future algorithm research and expertise, and with advice on whether Government regulation of algorithms is required and, if so, what options for regulation are available.

Encouraging industry transparency and accountability

There are four recommendations which focus on the responsibility of industry to protect Australian users. **Recommendations 5** and **11** are for the eSafety Commissioner to examine a range of issues relating to industry transparency and accountability in enforcing their terms of service and actively preventing specific harms. **Recommendations 16** and **17** propose additional proactive measures for digital services and technology manufacturers relating to privacy and safety settings and parental controls.

The Government agrees that industry should be held to account for the safety of their products and services. Consistent with this approach, the Online Safety Act (the Act) includes examples of matters that may be dealt with by industry codes or standards. The matters identified in Part 9 of the Act focus on dealing with illegal or restricted content.

Work on industry codes is underway. The first phase of the industry codes under the Act will focus on the most seriously harmful forms of content (such as child sexual exploitation and abuse material, and pro-terror content). One of these codes covers equipment manufacturers and suppliers and could include commitments relevant to parental controls. The second phase of these industry codes will focus on children's access to online pornography. This phase provides a further opportunity for equipment manufacturers and suppliers to commit to providing parental control and functionality.

The eSafety Commissioner will shortly be making a decision on whether the industry codes meet the registration requirements under the Act and provide appropriate community safeguards. If an industry code is not registered, the eSafety Commissioner can determine an industry standard for that section of the online industry. The Government will monitor the impact of the industry codes or industry standards and consider whether further action is needed to implement a mandatory requirement for technology manufacturers and providers to make available the option of parental control functionalities.

The Act also enables the Minister to determine the BOSE. The Online Safety (Basic Online Safety Expectations) Determination 2022 articulates the Government's expectations for social media services,

relevant electronic services and designated internet services accessible from Australia, with a focus on making sure these services take reasonable steps to keep Australians safe.

The Act allows the eSafety Commissioner to require providers of online services covered by the BOSE to report on steps they are taking to meet the expectations. This information can include the existence of terms of service, and the penalties that companies put in place for those breaching these terms of service. eSafety is also able to publish statements about the extent to which services are meeting the expectations.

The eSafety Commissioner's powers in relation to the BOSE may require reporting on matters related to a number of online safety concerns such as the recidivism of bad actors, pile-ons (or volumetric attacks) and harms across multiple platforms. DITRDCA will work closely with eSafety to advise Government on whether further regulatory interventions to address such issues are required.

Implementation of parental controls must also consider privacy impacts on children, and their right to autonomy. The report of the Privacy Act Review proposed enshrining a principle that recognises the best interests of the child and recommended the introduction of a Children's Online Privacy code modelled on the United Kingdom's Age Appropriate Design Code. A Children's Online Privacy code would clarify the principles-based requirements of the Privacy Act in more prescriptive terms, and would provide guidance on how the best interests of the child should be upheld in the design of online services. For example, assessing a child's capacity and establishing their age, limiting certain collections, uses and disclosures of children's personal information, default privacy settings, enabling children to exercise privacy rights, and balancing parental controls with a child's right to autonomy and privacy. Development of the Government's response to the Privacy Act Review report is currently underway.

Parliamentary oversight and a review of online safety

Parliamentary oversight

There are two recommendations in the Final Report which focus on Parliamentary oversight, including: to appoint a new Standing Committee on Internet, Online Safety and Technological Matters (**Recommendation 1**); and that this new committee inquire into the role of social media in relation to democratic health and social cohesion (**Recommendation 2**).

The Government agrees that Parliamentary oversight is important in the context of the broad ranging issues which arise in digital spaces. The Government will refer matters of public interest on regulation of online harms and the digital industry to the House of Representatives Standing Committee on Communications and the Arts. Utilising the existing standing committee will support the continuation of the longstanding nonpartisan approach taken across Government and Opposition on online safety, and leverage the existing structures which have been established for this very purpose. The Government also notes that since the Social Media and Online Safety Inquiry concluded, the following committees have been stood up or re-initiated inquiries relevant to online harms:

- Senate Select Committee on Foreign Interference through Social Media – Select Committee was re-established on 24 November 2022.
- Senate Standing Committee on Economics (References) – Inquiry into the influence of international digital platforms was referred on 26 September 2022.
- Joint Standing Committee on Electoral Matters (JSCEM) – Inquiry into the 2022 federal election was referred on 5 August 2022.
- Joint Committee on Law Enforcement – Inquiry into law enforcement capabilities in relation to child exploitation was re-initiated on 3 August 2022.

The JSCEM reviews all aspects of the conduct of each federal election and has previously reported on disinformation and misinformation in the electoral context. The Government also notes the Select Committee on Foreign Interference through Social Media will inquire into and report by 1 August 2023 on the risk posed to Australia's democracy by foreign interference through social media. In the previous Parliament, the committee published an interim report and a progress report prior to the 2022 federal election.

Review of the regulatory framework

There are four recommendations in the Final Report which focus on reviewing existing regulatory arrangements for the digital industry (**Recommendation 18**), including to consider: mandating platform transparency (**Recommendation 15**); introducing a single regulatory framework under the Online Safety Act to simplify regulatory arrangements (**Recommendation 19**); and to introduce a duty of care requirement (**Recommendation 20**). Additionally, there is one recommendation to consider the implementation of Safety by Design principles in future reviews of the Act (**Recommendation 9**).

The Government agrees that regulation and policy should be reviewed regularly, and notes that the Government is reviewing this in an ongoing fashion. There are a number of reviews and policy work already underway considering the range of regulatory frameworks that apply to digital platforms.

- The Senate Economics References Committee is conducting an inquiry into the Influence of international digital platforms, and is due to report by the last sitting day of 2023.
- The ACCC is conducting an inquiry into digital platforms services. The ACCC released its fifth interim report on 11 November 2022 which proposes measures to address competition and consumer issues. The Government released a consultation paper on 20 December 2022 in response to the report, and will be guided by a Treasury-led consultation process.
- The Privacy Act Review was released publicly on 16 February 2023. The Government will consult on the Report to inform the development of a Government response. The proposals in the Report are designed to ensure Australia's privacy framework responds to new challenges in the digital era, better aligns with global standards of information privacy protection and properly protects Australians' privacy.
- Under the National Strategy to Prevent and Respond to Child Sexual Abuse 2021–2030 (measure 13 of the Commonwealth Action Plan), AGD is reviewing Commonwealth child sexual abuse offences in the Criminal Code Act 1995 (Cth) to ensure that the legislative framework relating to child sexual abuse is comprehensive, reflects offending trends, and meets the needs of police and prosecutors.
- The Department of Home Affairs is establishing a stakeholder forum with digital industry representatives to work with industry on more effectively enacting Subdivision H of the Criminal Code Act 1995 (abhorrent violent material provisions) and to consult on future reforms.
- The Department of Home Affairs is also currently working towards the development of national principles and frameworks for data security, as part of the 2023-2030 Cyber Security Strategy.
- The Department of Home Affairs' Cyber Security Best Practice Regulation Taskforce is undertaking work relating to cyber security regulatory frameworks across the broader digital economy.

The Online Safety Act commenced in January 2022 and an independent review of its operation must commence by no later than January 2025. Recognising that the online world is evolving quickly, the Albanese Government commits to undertake and complete this review earlier than required and within

this term of Government so that Australia and our world-leading online safety framework remain fit for the changing online environment. The review will consider the operation of the existing framework, including industry codes and standards, and the BOSE reporting regime, as well as whether reforms are required to simplify regulatory arrangements including through the introduction of a duty of care requirement.

The outcomes of these processes will necessarily inform any future reform of legislation and regulation related to the digital industry.

Policy and regulatory coordination

Recommendations that the online safety framework be reviewed also sought to address evidence regarding a perceived lack of coordination across Government. As the Inquiry demonstrated, issues surrounding online harms are complex and span across a range of government portfolios, requiring a coordinated response.

Responsibility for specific online harms is split in line with responsibility for harms offline. For example, relevant to the issues raised in the Inquiry, policy responsibility for online safety generally sits with the Minister for Communications; responsibility for online defamation, human rights, anti-discrimination and racial hatred, and privacy sits with the Attorney-General; and cyber security responsibility sits with the Minister for Home Affairs. The eSafety Commissioner is Australia's dedicated online safety regulator responsible for implementing the online safety regulatory framework and has a statutory role in driving education, research and national coordination relating to online safety.

To support a streamlined and cohesive approach to the regulation of digital platforms, the ACMA, the ACCC, the OAIC, and the office of the eSafety Commissioner have formed the DP-REG. DP-REG is an initiative of these four regulators to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms. This includes considering how competition, consumer protection, privacy, online safety and data issues intersect and seeking to improve regulatory consistency across digital platforms while retaining domain expertise.

To further strengthen whole-of-government coordination efforts and complement the work of the DP-REG, the Government will convene a bi-annual meeting of Ministers with responsibility for online harms. This will support identification of opportunities for cooperation across relevant portfolios, ensuring alignment of resources and educational, awareness-raising, research and prevention activities.

Conclusion

The Australian Government appreciates the opportunity to provide its response to the report of the House Select Committee on Social Media and Online Safety. We would like to thank members of the Select Committee, in particular the Chair, for the constructive and bipartisan nature in which this Inquiry was conducted. We would also like to thank every witness who provided insights into their own experiences of online harms. The valuable evidence provided by these witnesses, and the evidence contained in the Committee's Final Report, will inform the Government's continued efforts to keep all Australians safe from online harms.

Appendix

Australia's online safety framework

Online Safety Act 2021

Australia's *Online Safety Act 2021* (the Act), which commenced in January 2022, supports Australians online by providing the eSafety Commissioner with powers to address cyberbullying of children, online cyber abuse of adults, illegal and restricted content, and the non-consensual sharing of intimate images. The Act makes online service providers more accountable for the online safety of the people who use their services through the Basic Online Safety Expectations (BOSE) and the development of industry codes or industry standards.

BOSE

While there is a role for government, users and the community, the primary responsibility to create safe online spaces sits with industry. The BOSE articulate the minimum safety expectations of online service providers, establishing a benchmark for online service providers to take proactive steps to protect the community from abusive conduct and harmful content online. The eSafety Commissioner has the power to require certain service providers to report on their compliance with these Expectations.

Industry codes

The Act also requires new codes to be developed by industry and considered by the eSafety Commissioner for registration. The aim of the industry codes is for the online industry to do more to regulate the access, distribution and exposure of end-users in Australia to illegal and restricted online content – 'class 1' and 'class 2' content – under the online content scheme. Examples of material that may be covered by the industry codes includes content showing sexual abuse of children and young people, acts of terrorism through to content which is inappropriate for children, such as online pornography. If the eSafety Commissioner finds the draft industry codes do not provide appropriate community safeguards and are therefore deficient, the eSafety Commissioner may determine industry standards.

Industry codes or industry standards apply to participants of 8 key sections of the online industry including providers of: social media; email; messaging; gaming; dating; search engine and app distribution services, and internet and hosting service providers; manufacturers and suppliers of equipment used to access online services; and providers that install and maintain the equipment.

Review of the Online Safety Act

Within three years after the commencement of the Act, an independent review of the operation of the Act and legislative rules must be conducted. This review is to consider whether any amendments to the Act or the rules are required.

Terms of Reference

On 1 December 2021, the House of Representatives established the House Select Committee on Social Media and Online Safety (the Committee) to inquire into:

a) the range of online harms that may be faced by Australians on social media and other online platforms, including harmful content or harmful conduct;
b) evidence of:
    i. the potential impacts of online harms on the mental health and wellbeing of Australians;
    ii. the extent to which algorithms used by social media platforms permit, increase or reduce online harms to Australians;
    iii. existing identity verification and age assurance policies and practices and the extent to which they are being enforced;
c) the effectiveness, take-up and impact of industry measures, including safety features, controls, protections and settings, to keep Australians, particularly children, safe online;
d) the effectiveness and impact of industry measures to give parents the tools they need to make meaningful decisions to keep their children safe online;
e) the transparency and accountability required of social media platforms and online technology companies regarding online harms experienced by their Australian users;
f) the collection and use of relevant data by industry in a safe, private and secure manner;
g) actions being pursued by the Government to keep Australians safe online; and
h) any other related matter.

Over the course of the inquiry, the Committee received 107 submissions (including supplementary submissions) and held 11 public hearings with 55 witnesses.

The final report was tabled on 15 March 2022, with the Committee making 26 recommendations and Labor members made a further 7.

List of Recommendations

Recommendation 1: The Committee recommends that the Australian Government propose the appointment of a House Standing Committee on Internet, Online Safety and Technological Matters, from the commencement of the next parliamentary term.

Recommendation 2: The Committee recommends that, subject to Recommendation 1, the Australian Government propose an inquiry into the role of social media in relation to democratic health and social cohesion, to be referred to the aforementioned committee or a related parliamentary committee.

Recommendation 3: The Committee recommends that the eSafety Commissioner undertakes research focusing on how broader cultural change can be achieved in online settings.

Recommendation 4: Subject to the findings in Recommendation 3, the Committee recommends that the Australian Government establishes an educational and awareness campaign targeted at all Australians, focusing on digital citizenship, civics and respectful online interaction.

Recommendation 5: The Committee recommends that the eSafety Commissioner examine the extent to which social media companies actively prevent:

- recidivism of bad actors
- pile-ons or volumetric attacks; and
- harms across multiple platforms.

The eSafety Commissioner should then provide the Australian Government with options for a regulatory framework, including penalties for repeated failures.

Recommendation 6: The Committee recommends that the Office of the eSafety Commissioner be provided with adequate appropriations to establish and manage an online single point of entry service for victims of online abuse to report complaints and be directed to the most appropriate reporting venue, dependent on whether their complaints meet the requisite threshold, and in consideration of a variety of audiences such as children, parents/carers, women, people from culturally and linguistically diverse backgrounds, and other relevant vulnerable groups.

Recommendation 7: The Committee recommends that the Australian Government refer to the proposed House Standing Committee on Internet, Online Safety and Technological Matters, or another committee with relevant focus and expertise, an inquiry into technology-facilitated abuse, with terms of reference including:

- The nature and prevalence of technology-facilitated abuse;
- Responses from digital platforms and online entities in addressing technology-facilitated abuse, including how platforms can increase the safety of their users; and
- How technology-facilitated abuse is regulated at law, including potential models for reform.

Recommendation 8: The Committee recommends that the Australian Government significantly increase funding to support victims of technology-facilitated abuse, through existing Australian Government-funded programs. This should include additional funding for specialised counselling and support services for victims; and be incorporated in the next National Action Plan to End Violence Against Women and Children 2022-2032.

Recommendation 9: The Committee recommends that future reviews of the operation of the *Online Safety Act 2021* take into consideration the implementation of the Safety by Design Principles on major digital platforms, including social media services and long-standing platforms which require retrospective application of the Safety by Design Principles.

Recommendation 10: The Committee recommends that the Department of Infrastructure, Transport, Regional Development and Communications, in conjunction with the eSafety Commissioner and the Department of Home Affairs, examine the need for potential regulation of end-to-end encryption technology in the context of harm prevention.

Recommendation 11: The Committee recommends that the eSafety Commissioner, as part of the drafting of new industry codes and implementation of the Basic Online Safety Expectations:

- Examine the extent to which social media services adequately enforce their terms of service and community standards policies, including the efficacy and adequacy of actions against users who breach terms of service or community standards policies;
- Examine the potential of implementing a requirement for social media services to effectively enforce their terms of service and community standards policies (including clear penalties or repercussions for breaches) as part of legislative frameworks governing social media platforms, with penalties for non-compliance; and
- Examine whether volumetric attacks may be mitigated by requiring social media platforms to maintain policies that prevent this type of abuse and that require platforms to report to the eSafety Commissioner on their operation.

Recommendation 12: The Committee recommends that the eSafety Commissioner examine the extent to which social media companies actively apply different standards to victims of abuse depending on whether the victim is a public figure or requires a social media presence in the course of their employment, and provides options for a regulatory solution that could include additions to the Basic Online Safety Expectations.

Recommendation 13: The Committee recommends that the eSafety Commissioner, in conjunction with the Department of Infrastructure, Transport, Regional Development and Communications and the Department of Home Affairs and other technical experts as necessary, conduct a review of the use of algorithms in digital platforms, examining:

- How algorithms operate on a variety of digital platforms and services;
- The types of harm and scale of harm that can be caused as a result of algorithm use;
- The transparency levels of platforms' content algorithms;
- The form in which regulation should take (if any); and
- A roadmap for Australian Government entities to build skills, expertise and methods for the next generation of technological regulation in order to develop a blueprint for the regulation of Artificial Intelligence and algorithms in relation to user and online safety, including an assessment of current capacities and resources.

Recommendation 14: The Committee recommends that the eSafety Commissioner require social media and other digital platforms to report on the use of algorithms, detailing evidence of harm reduction tools and techniques to address online harm caused by algorithms. This could be achieved through the mechanisms provided by the Basic Online Safety Expectations framework and Safety by Design assessment tools, with the report being provided to the Australian Government to assist with further public policy formulation.

Recommendation 15: The Committee recommends that, subject to Recommendation 19, the proposed Digital Safety Review make recommendations to the Australian Government on potential proposals for mandating platform transparency.

Recommendation 16: The Committee recommends the implementation of a mandatory requirement for all digital services with a social networking component to set default privacy and safety settings at their highest form for all users under 18 (eighteen) years of age.

Recommendation 17: The Committee recommends the implementation of a mandatory requirement for all technology manufacturers and providers to ensure all digital devices sold contain optional parental control functionalities.

Recommendation 18: The Committee recommends that the Department of Infrastructure, Transport, Regional Development and Communications conduct a Digital Safety Review on the legislative framework and regulation in relation to the digital industry. The Digital Safety Review should commence no later than 18 months after the commencement of the Online Safety Act 2021, and provide its findings to Parliament within twelve (12) months.

Recommendation 19: The Committee recommends that, subject to Recommendation 18, the Digital Review examine the need and possible models for a single regulatory framework under the Online Safety Act, to simplify regulatory arrangements.

Recommendation 20: The Committee recommends that the Digital Review include in its terms of reference:

- The need to strengthen the Basic Online Safety Expectations to incorporate and formalise a statutory duty of care towards users;
- The scope and nature of such a duty of care framework, including potential models of implementation and operation;
- Potential methods of enforcement to ensure compliance, including penalties for non-compliance; and
- The incorporation of the best interests of the child principle as an enforceable obligation on social media and other digital platforms, including potential reporting mechanisms

Recommendation 21: The Committee recommends that the eSafety Commissioner:

- Increase the reach of educational programs geared at young people regarding online harms, with a particular focus on reporting mechanisms and the nature of some online harms being a criminal offence;
- Formalise a consultation and engagement model with young people through the Australian Government's Youth Advisory Council in regards to educational themes and program delivery; and
- Report to the Parliament on the operation and outcomes of the program, including research identifying whether this has resulted in a reduction in online harm for young people.

Recommendation 22: The Committee recommends that the eSafety Commissioner work in consultation with the Department of Education, Skills and Employment to design and implement a national strategy on online safety education designed for early childhood, and primary school-aged children, and secondary school-aged young people, including:

- A proposed curriculum, informed by developmental stages and other relevant factors;
- Potential methods of rollout, including consultation and engagement with children, young people, child development and psychology experts, digital education experts and other specialists in online harm; and
- A roadmap provided to parents of these age groups detailing methods of addressing online harm.

Recommendation 23: The Committee recommends that the eSafety Commissioner design and administer an education and awareness campaign aimed at adults, particularly in relation to vulnerable groups such as women, migrant and refugee groups, and people with disabilities, with a focus on the eSafety Commissioner's powers to remove harmful content and the mechanisms through which people can report harmful content and online abuse.

Recommendation 24: The Committee recommends that the Australian Government work with states and territories to ensure that relevant law enforcement agencies are appropriately trained on how to support victims of online harm. This should include trauma-informed approaches as well as a comprehensive understanding of police powers and other relevant avenues, such as the relevant powers of the eSafety Commissioner.

Recommendation 25: The Committee recommends that the Australian Government review funding to the eSafety Commissioner within twelve (12) months to ensure that any of the Committee's recommendations that are agreed to by the Government and implemented by the Office of the eSafety Commissioner are adequately and appropriately funded for any increased resource requirements.

Recommendation 26: The Committee recommends that the Online Safety Youth Advisory Council, via the eSafety Commissioner, provide a response to this report and its recommendations within six (6) months of its establishment and full membership.

Developing the Government response

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) coordinated the development of the Australian Government's response. DITRDCA sought input from the following Commonwealth agencies:

- the Attorney-General's Department;
- Australian Communications and Media Authority;
- Australian Competition and Consumer Commission;
- Australian Criminal Intelligence Commission;
- Australian Electoral Commission;
- Australian Federal Police/Australian Centre to Counter Child Exploitation;
- Australian Human Rights Commission;
- Australian Institute of Criminology;
- Australian Signals Directorate;
- Department of Education;
- Department of Finance;
- Department of Home Affairs;
- Department of Industry, Science and Resources;
- Department of the Prime Minister and Cabinet;
- Department of Social Services;
- Department of the Treasury;
- Digital Transformation Agency;
- eSafety Commissioner;
- National Indigenous Australians Agency; and
- Office of the Australian Information Commissioner.