Report of the Independent Legal Examination into Banning Children's Access to Social Media

September 2024

Prepared by the Honourable Robert French AC

REPORT

Table of Contents

The Hon Robert S French AC

Suite 2, Level 13
Allendale Square
77 St George's Terrace
Perth WA 6000

T: +61 8 92212803
E: sulcsj@13french.com

8 September 2024

Premier of South Australia
State Administration Centre
200 Victoria Square
ADELAIDE SA 5000

Dear Premier

Re: Legal Examination of Proposed Age-Based Social Media Restrictions

Thank you for affording me the opportunity to assist the Government of South Australia in providing my views on a legislative model to give effect to a ban on access to social media services by children under the age of 14, and requiring parental consent for access by 14 and 15 year old children.

In preparing the Report, I have taken as my premise the policy setting adopted by the South Australian Government. I have endeavoured, however, to have regard to the complex and dynamic setting in which any legislation of this kind must operate.

I have prepared a draft Bill which is not intended to be definitive but indicative of the shape of legislation which could give effect to your desired policy.

I am grateful for the considerable support I have received from officers of the Department of the Premier and Cabinet and other officers of the South Australian Government. I am also grateful to the many people, including statutory officers of the South Australian Government and of the Commonwealth, who have given me the benefit of their experience and expertise in my examination.

The social issue with which you and your Government are engaging is one of global concern. For my own part, I would hope that the South Australian initiative leads to some form of coherent national response.

I provide my Report.

Yours sincerely

The Hon Robert French AC

I. Introduction

This Report to the Government of South Australia follows a legal examination to determine whether the State of South Australia could legislate a ban on access to social media services by children who have not attained the age of 14 and to restrict access to social media services by children between the ages of 14 and 16 by requiring parental consent to their access. The Report also considers a legislative model for achieving that end.

The Report sets out the Terms of Reference and Conclusions and Proposal along with a draft Bill which is presented as a working document. The Draft Bill sets out an indicative model for legislation which might be enacted to give effect to the Government policy objectives. It would require review by Parliamentary Counsel and consideration by the Government's own legal advisors before being introduced into Parliament.

The Conclusions and Proposal follow an examination of Commonwealth legislation and regulatory schemes in other countries. That examination has also involved consideration of relevant literature and inputs received from a number of persons, including State and Commonwealth officers, academics, and social media service providers, young people and others with relevant interests and expertise. A list of meetings, mostly online, convened for the purposes of the Examination is included after this Introduction. It has not been possible to include in this Report a detailed analysis of each contribution. However, the range of views presented in the Examination, is reflected in the Report. All contributors provided valuable insights, albeit there was a degree of convergence of views for and against a legislative ban. The Examination was also ably supported by officers of the Department of the Premier and Cabinet of South Australia and other officers who provided briefing materials, reached out to various interested parties and arranged meetings and reviewed draft chapters.

As stated to all contributors to this process, the purpose of this Report is not to canvass the merits of the policy setting adopted by the Government of South Australia, but to examine a legislative approach to its implementation. In developing a legislative approach, consideration has been given, in the light of views expressed to the Examination, to a mechanism for preserving access to beneficial social media services. Consideration has also been given to ensuring, so far as possible, the practical workability of the legislation from the perspective of social media service providers who would be subject to its new statutory duties in South Australia.

The Report proposes that the restriction to access could be effected by the imposition on social media service providers of two statutory duties of care. The first would be a duty to prevent access to social media services by children under the age of 14 and by children between 14 and 16 years without parental consent. There would necessarily be a 'reasonable steps' defence to a contravention of that duty. The second, would be a duty to take reasonable steps to prevent the prohibited access. The term 'social media service' is defined broadly based on the definition in the Commonwealth legislation, the *Online Safety Act* 2021 (Cth) ('***Online Service Act***') but covering other services of concern. There are options which would be available to the Government in defining 'social media service' more or less broadly. Those options are indicated in the last Chapter.

The concept of 'exempt social media' is introduced to enable the reach of the legislation to be appropriately calibrated. The proposed duties would not apply with respect to exempt social media services. The criteria for determining an exempt social media service and guidance as to what might constitute 'reasonable steps' to comply with the statutory duties would have to be developed by the regulator drawing upon the expertise and experience of the Commonwealth eSafety Commissioner's office, age assurance providers, social media service providers, independent experts and other stakeholders. Exempt social media services would be services which pose little or little significant risk to children. They would, for example, include social media services provided by educational and health authorities. Social media services serving closed community support groups and social media services access to which is controlled by an adult, such as a classroom teacher using the service for teaching purposes.

Enforcement of the first duty would be primarily in response to complaints. Enforcement of the second duty would be based upon regulatory inspection, spot-testing and information gathering and periodic reporting from social media service providers.

A range of enforcement mechanisms of the kind generally applicable in regulatory schemes can be provided for in the legislation up to and including civil penalties. A bespoke monetary sanction, where there has been a breach which would not warrant the imposition of a civil penalty, would be a compensation order which would require the payment of a sum into a compensation fund which would be used for research and policy development relevant to the purposes of the legislation and also be a source of discretionary compensation payments to a child adversely affected by a breach of one or other of the statutory duties. The compensation payment mechanism would be analogous to criminal injuries compensation schemes which are

in place in various States. In addition, it is proposed that the breach of a duty resulting in mental or physical harm to a child be a statutory tort for which damages could be recoverable by action taken in the name of the child and, alternatively, by action taken by the Regulator on behalf of the child.

The proposal allows for the establishment of a standalone State Regulator or conferral of functions on an existing State regulator. Another alternative, with the agreement of the Commonwealth, would be conferral of functions under State laws on the National eSafety Commissioner, such conferral necessarily being supported by a law of the Commonwealth.

The Report suggests a mechanism for ongoing research and policy development in a difficult and rapidly changing regulatory environment.

Constitutional issues have been considered and the proposed legislative model should be within the legislative power of the South Australian Parliament. That said, the challenges of compliance with and enforcement of a law restricting access by children in one State and not all are strong indications of the need for a national approach if that can be achieved.

Terms of Reference and Scope of Examination

The terms of reference as published by the Government of South Australia included introductory paragraphs and a list of matters to be considered in the Examination.

The introductory paragraphs set out the policy framework adopted by the South Australian Government within which the Legal Examination was to be conducted. The introductory paragraphs were as follows:

> The use of social media including exposure to inappropriate, illegal and restricted content and cyber bullying is having a harmful effect on the wellbeing and mental health of children.
>
> The existing safeguards to protect children from the negative impacts of social media are not in step with community expectations. The objective of the South Australian Government is to reduce this harm by pursuing legislative and regulatory reforms as a matter of priority.
>
> The challenges associated with regulating social media platforms are complex and multifaceted, particularly regarding jurisdictional responsibility. To enable the South Australian Government to better protect children from the negative impacts of social media, the Premier is commissioning an independent legal examination into how to ban children from having social media accounts.
>
> Former High Court Chief Justice, the Honourable Robert French, AC will lead the examination into how legislation, regulation and supporting technology can be utilised to prohibit social media access for children aged under 14 and require parental consent for children aged 14 and 15 in South Australia.

The substantive topics to be considered in the Examination were listed as follows:

> The Examiner will consider:
>
> - How South Australia can achieve the objective of social media prohibition for children within Australia's constitutional framework.
> - The existing legislative and regulatory landscape in South Australia including effectiveness of current legislative and regulatory levers for limiting access to social media for children.
> - Opportunities for legislative or regulatory reform in South Australia to prevent access to social media accounts for children under 14 and require parental consent for children aged 14 and 15.
> - How actions taken in South Australia to limit social media access for children could be effectively enforced.
> - How existing technology to limit access to social media such as 'age assurance' mechanisms could be utilised to complement legislative and/or regulatory change.

- How examples of other jurisdictions that have implemented limitations on social media access for children could be applied in South Australia.
- Any other matters as determined by the Examiner.

A coda to the substantive Terms of Reference set out matters to which the Examiner is to have due regard as follows:

> Without limiting the scope of the inquiry or the scope of any recommendations arising out of the examination, the Examiner will also have due regard to:
>
> - Other relevant reviews underway into how government can limit social media access for young people in other jurisdictions including the Commonwealth Government.
> - Broad consultation including with experts, social media platform providers and any other relevant stakeholders.

The Terms of Reference stated that the Final Report will be submitted to the Premier and Cabinet.

Secretariat and other required support was provided by the Department of the Premier and Cabinet and the Attorney-General's Department.

In undertaking the Examination, I have met with a number of statutory officers, experts and interested parties. A list of those persons is set out below.

III List of Meetings

1.	Professor Marilyn Bromberg, **University of Western Australia** (2 May 2024)
2.	Professor David Plater and Professor John Williams AM, **University of Adelaide** and **South Australian Law Reform Institute** (8 July 2024) – Online
3.	Ms Helen Connolly, **Commissioner for Children and Young People** (15 July 2024) – Adelaide
4.	Ms Sonya Ryan OAM, **The Carly Ryan Foundation** (15 July 2024) – Online
5.	Ms Taimi Allan, **SA Mental Health Commissioner** (15 July 2024) – Online
6.	**SA Department for Education** Officials (15 July 2024) – Adelaide
7.	Dr Mohammed Usman, **Child and Adolescent Mental Health Service** (15 July 2024) – Adelaide
8.	Dr John Brayley, Chief Psychiatrist, Associate Professor Melanie Turner and Mr Dave Thompson **Office of the Chief Psychiatrist** (15 July 2024) – Online and in person
9.	Ms Julie Inman Grant **eSafety Commissioner**; Ms Kathryn King, Ms Kelly Tallon, Ms Mariesa Nicholas, Mr Mike Skwarek and Mr Dom Tubier, **Office of the eSafety Commissioner** (16 July) – Sydney
10.	Ms Anne Hollands, Ms Susan Nicolson and Ms Susan Newell, **National Children's Commissioner** (17 July 2024) – Sydney
11.	Ms Delia Rickard PSM, Ms Rebecca Day, Ms Anthea Belessis, and Mr Andrew Irwin Online Safety Act Review (19 July 2024) – Online
12.	Dr Danielle Einstein, **Clinical Psychiatrist and Adjunct Fellow** (5 August 2024) – Online
13.	Ms April Lawrie and Ms Alisha Staines, **Commissioner for Aboriginal Children and Young People** (6 August 2024) – Online
14.	Ms Shona Reid**, Guardian for Children and Young People** (7 August 2024) – Online
15.	**eSafety Youth Council** (8 August 2024) – Online
16.	Ms Lucinda Longcroft and Ms Rachel Lord, **Google and YouTube** (12 August) – Online
17.	Mr Iain Corby, **Age Verification Providers Association** (14 August 2024) – Online
18.	Mr Henry Turnbull and Mr Ben Au, **Snap Inc** (15 August 2024) – Online
19.	Ms Ella Woods-Joyce and Ms Amelia Crawford **TikTok** (19 August 2024) – Online
20.	Ms Mia Garlick, **Meta** (19 August 2024) – Online
21.	Ms Maggie Rutjens, **Office for Autism** (21 August 2024) – Online

Professor Marilyn Bromberg, University of Western Australia

Meeting Date: 2 May 2024 (Online)

Attendees:

- Professor Marilyn Bromberg, University of Western Australia

Topics Discussed:

- Social media issues generally in relation to children — risks and benefits — regulation of social media platforms
- Ways in which restrictions may be avoided — e.g. VPNs.

South Australian Law Reform Institute

Meeting Date: 8 July 2024

Attendees:

- Mr John Williams AM, Professor, University of Adelaide
- Mr David Plater, Professor, University of Adelaide

Topics Discussed:

- Whether a statutory tort would better suit as a legal mechanism to prevent providers from allowing children to access social media — practicalities of establishing such a tort — possibility of class actions — enforcement of damages
- Constitutional limitations — s 92, s 117 — implied freedom of political communication.

South Australian Commissioner for Children and Young People

Meeting Date: 15 July 2024

Attendees:

- Ms Helen Connolly, Commissioner

Topics Discussed:

- The Commissioner's views including her views on the ineffectiveness of a ban on children's access.
- The ambit of the 'social media' definition and the importance of legislating in such a way that allows for platforms which facilitate learning and the school environment, such as 'EdTech', 'Class Dojo' and 'Seesaw'.
- The emerging trend of social media access among children 'aging down' with the start of High School being reduced to Year 7 within South Australia.
- The discrepancies between schools surrounding the use of phones by students in school and the implementation of such measures on a school-by-school basis in practice.
- Whether many children-focused government representatives have attempted pursuing regulation in the online space.
- The potential interaction of the proposed legislation with the Convention on the Rights of the Child, particularly the rights associated with Art 12, regarding children's freedom of expression and Art 17, regarding obligations to allow children access to information.

The Carly Ryan Foundation

Meeting Date: 15 July 2024

Attendees:

- Ms Sonya Ryan OAM, Founder and Chief Executive Officer

Topics Discussed:

- Ms Ryan's support for the implementation of a ban in South Australia and her wish for the form of legislation to emulate that of the recent United States *Kids Off Social Media Act*.

- The need for regulation to target the social media platform itself as the only effective means of implementation, as is evidenced by the initiatives of Florida and Arkansas within the United States.

- The fundamental role of a proposed social media ban in providing parental support and empowering parents to implement a shield of protection surrounding their children's access.

- The implementation of age assurance and age verification methods and the overarching preference to delegate the type of age assurance to be decided at the social media provider's discretion.

- The potential appointment of the eSafety Commissioner as the regulator.

- Identified mental health services for children as a category of platform which should be preserved if possible.

South Australian Mental Health Commissioner

Meeting Date: 15 July 2024

Attendees:

- Ms Taimi Allan, Commissioner

Topics Discussed:

- The potential for exempting services which are vital to the mental health of children.
- The importance of implementing a workable definition of 'social media', particularly with regard to the pace of development in the mental health and wellbeing application space.
- Positive experiences of users when engaging in mental health applications which implemented a mechanism, presumably a chat function, to engage with others, pursuant to empirical research.
- Whether mental health apps could be categorised as 'exempt'.
- The wellbeing and mental health applications 'Headspace' and 'Sane' appropriateness for children.
- The displacement of children from social media apps to gaming platforms or other problematic online spaces. The need to expand the definition of social media to anticipate such a movement.
- The role such a ban would play in supporting parents in the course of their own endeavours to keep their children off social media.
- The importance of framing such a ban as a public health concern, akin to smoking and drinking.

South Australian Department for Education

Attendees:

- Mr Dan Hughes, Chief Information Officer
- Ms Deala Zahr, Director Strategy and Operations, ICT Strategic Operations and Reform
- Mr Matt Jessett, A/Director Curriculum Development, Curriculum & Learning Division
- Mr Harry Manatakis, A/Director Engagement and Wellbeing
- Ms Katie Sciberras, Assistant Director, Behaviour Support Reform

Topics Discussed:

- The types of platforms which should be preserved for the use of children, primarily in the areas of educational services, health diagnostic and mental health.

- The Department's initiative towards centralising technology and internet services, through providing internet connection to schools and pre-schools across South Australia.

- Child-specific protections, such as limiting access tools and filtering capabilities.

- The availability of Office 365 to children across the sector and potential preservation of this as a fundamental educational platform. While the Office Suite is not conventionally understood as a social media service, there are collaboration functions worth noting.

- YouTube being utilised in the school environment to share short, educational videos.

- There are many purpose-built social media platforms for the school environment, like Schoolology. Individual departmental schools are able to sign up to use these platforms for student collaboration.

Child and Adolescent Mental Health Services

Meeting date: 15 July 2024.

Attendees:

- Dr Mohammed Usman, Child Psychiatrist and Clinical Director.

Topics Discussed:

- Social media services for use in the context of mental health care for young people.
- Prevalence of the use of social media, and alternatives to social media services for accessing mental health care for children under 14.
- Effectiveness of internet-based mental health services for young people, outside of social media.
- Social media is the easiest way to reach most young people. Is there an alternative that will result in equal accessibility of services for young people?
- The harms caused to young people by social media: addictive behaviour and cyberbullying.
- The benefits of social media for culturally and linguistically diverse communities.

Office of the Chief Psychiatrist, South Australia

Meeting date: 15 July 2024.

Attendees:

- Dr John Brayley, Chief Psychiatrist
- Associate Professor Melanie Turner, Deputy Chief Psychiatrist
- Mr Dave Thompson, Principal Project Officer, Suicide Prevention

Topics Discussed:

- Utility of a clear cyber safety strategy within legislation to prevent harm to young people online.
- The importance of education: children will eventually have access, and therefore need to know how to conduct themselves safely online.
- The 'Werther effect' of negative reporting of suicide and self-harm online, and the 'Papageno effect' of safe and responsible reporting of harmful behaviours.
- Using knowledge of psychological effects to put diversions and safeguards directly into algorithms.
- The issues children have and kinds of harms they face from social media.
- Children will copy the behaviour they see displayed in social media content, such as self-harm, eating disorders, and drug intake.
- The idea of using content ratings (e.g. G, PG, M) to streamline what kinds of content children can view.
- There are means of socialising children outside of social media — it is not necessary for this purpose.
- Platforms that only provide chat functions are safer than platforms that offer access to short form content, though they are not perfect.
- Balancing age and developmental capacity.

Office of the eSafety Commissioner

Meeting Date: 16 July 2024.

Attendees:

- Ms Julie Inman Grant, eSafety Commissioner
- Ms Kathryn King, General Manager, Technology and Strategy Division
- Ms Kelly Tallon, Executive Manager, Industry Compliance and Enforcement
- Ms Mariesa Nicholas, Manager, Strategy, Engagement & Research
- Mr Mike Skwarek, Manager, BOSE, Industry Regulation and Legal
- Mr Dom Tubier, Acting Head of Legal Services

Topics Discussed:

- The crucial importance of teaching children and parents digital literacy.
- The logistics of policy implementation: defining social media, what will be banned, the possibility of a separate regulator.
- The creation of a national scheme: the possibility of conferring State power to regulate social media on the Commonwealth, and the importance of a scheme with uniform standards and requirements Australia wide.
- The possibility of government taking a proactive strategic role to encourage the development of alternative, child friendly social media services.
- Safety by design: protection of children on social media by safety protections and risk assessment embedded in the platforms.
- Privacy issues involved with requiring users to supply ID verification to platforms to facilitate age assurance.
- Collection of data to understand the 'lay of the land' about how young people are using social media.
- The utility of a ban vs imposing a duty of care on social media platforms not to allow users under 14.

- The ephemeral nature of social media and melting pot of services — regulatory difficulties.
- Enforcement of Australian penalties against social media companies incorporated overseas.
- The viability of international networks of regulators to enforce penalties. Working with the rest of the world the only way forward for online safety.
- The importance of a broad definition of social media and a duty of care that places the onus on the social media platforms.
- Concern that a ban will disincentivise children from seeking help when facing harm online.

National Children's Commissioner

Meeting Date: 17 July 2024.

Attendees:

- Ms Anne Hollands, National Children's Commissioner
- Ms Susan Nicolson, Director Children's Rights
- Ms Susan Newell, Senior Policy Officer Children's Rights

Topics Discussed:

- The utility of imposing a duty of care on social media providers as opposed to a ban.
- Including a defence for social media platforms that have taken all reasonable steps to facilitate online safety in accordance with existing technologies.
- Exempting certain social media services to protect the benefits of social media use for children.
- The inequity of restrictions falls most heavily on marginalised children, children with complex needs and children experiencing poverty. Children without access to a caring adult will fall through the cracks.
- Whether a ban will disincentivise children to communicate with parents and carers about online harm.
- Discussion around if online gaming will be captured in the social media definition and how it would be included if it falls into the notion of an interactive electronic service.
- The importance of consulting with young people about these issues that will affect them.
- Certain groups of children rely on social media access for their wellbeing and self-identity (e.g. LGBTQIA+).
- The effect of a ban on First Nations communities.

Statutory Review of the Online Safety Act

Meeting Date: 22 July 2024.

Attendees:

- Ms Delia Rickard PSM, Online Safety Act Reviewer
- Ms Rebecca Day, Secretariat / Director, Online Safety Strategy and Research
- Ms Anthea Belessis, Secretariat
- Mr Andrew Irwin, Assistant Secretary, Online Safety Branch

Topics Discussed:

- The ways the duty of care may be approached.
- The eight definitional categories of online services under the *Online Safety Act* (Cth). What kinds of services constitute social media?
- Legislating to distinguish between the benefits and harms of social media.
- Defining the duty of care to encourage social media platforms to take proactive action on online safety. The importance of putting the onus on the platforms.
- Age assurance is not perfect but will ultimately be useful.

Dr Danielle Einstein, Clinical Psychiatrist and Adjunct Fellow at Macquarie University

Meeting Date: 5 August 2024.

Attendees:

- Dr Danielle Einstein, Clinical Psychologist and Adjunct Fellow

Topics Discussed:

- Whether the mental health services offered through social media can still be delivered through the internet without social media.
- Do we need additional rules for advertising to children through social media?
- The correlation between mental health struggles and the inability to handle uncertainty. Social media provides immediate access to people we feel safe with — people that can lessen uncertainty.
- At what age is it appropriate for children to develop the skills to broadcast themselves to many people?
- Direct correlation between young children using social media and mental health struggles.
- No beneficial upside to social media that warrants the Safety by Design principle.
- The ephemeral and dopamine inducing nature of social media is harmful to memory, attention span, and the ability to think ahead.
- There are better ways to provide young people with mental health support than social media: social media only teaches them to be dependent.
- Possibility of including a moderation mechanism to regulate what aspects of social media children can access.
- Social media is designed to grab our attention. The dopamine hits gleaned from others reacting to their posts can be all consuming for children.

- Social media has no benefits for any group that outweighs the harm it threatens. Any support that can be provided online is more effective offline.
- The link between social media and school refusal.
- Raising children in an environment where they are completely dependent on devices for entertainment and support for what is harming them. The issue is unfettered access.
- If we are going to choose moderation over a ban, there needs to be time limits on how long children can use them for.

Commissioner for Aboriginal Children and Young People

Meeting date: 6 August 2024

Attendees:

- Ms April Lawrie, Commissioner
- Ms Alisha Staines

Topics Discussed:

- The many beneficial uses of social media platforms in remote communities — sharing information, keeping connected, education, mental health, and wellbeing.
- The health impacts of online gaming addiction.
- There are many apps used in Aboriginal communities which range from the normal ones like Facebook, to administrator regulated apps, where communities stay connected.
- Educating kids to use the apps properly and manage the risks, report racism and abuse.

Guardian for Children and Young People

Meeting date: 7 August 2024

Attendees:

- Ms Shona Reid, Guardian

Topics Discussed:

- Children always find a way around restrictions and the risk is heightened.
- The negative impact if points of connection, tools and assets are removed, including mental health and wellbeing.
- Preserving the rights of children in favour of educating them on online safety to ensure rights are upheld.
- Concerns of the Guardian's capacity to reach out to children will be inhibited by the ban as this is the way many children in care contact the office.
- Many children in care are reliant on social media to maintain a connection with their family and create peer connections.
- There are higher and significant risks to the child when some situations are controlled by parents, especially in family violence or exploitation situations.

eSafety Youth Council

Meeting date: 8 August 2024

Attendees:

- Ms Nicky Sloss, Manager, Education Services
- Ms Shasha McKinnon, eSafety Youth Council Support Team
- Ms Emma O'Hare, eSafety Youth Council Support Team
- eSafety Youth Council Members: Arjun, Elena, Elliot, Minh, and Tracey

Topics Discussed:

- Risks and benefits of social media access and use, particularly in relation to LGBTQIA+ teens, First Nations teens and young people with a disability.
- The scrolling aspect of social media and its impact on attention spans, addictiveness of those under 14.
- Importance of messaging apps for communication and social connections between teens.
- Many messaging apps could be recognised as social media apps, such as WeChat and Discord, as users can talk to who they want.
- The Youth Council's view on YouTube and YouTube Kids, and how these platforms have more opportunities than risks, as they offer a broad range of topics for learning and study at school. Additionally, YouTube only offers what a user looks for, rather than the likes of Instagram where the content is not actively sought out.

Google and YouTube

Meeting Date: 12 August 2024

Attendees:

- Ms Lucinda Longcroft, Director, Government Affairs and Public Policy
- Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy

Topics Discussed:

- Whether YouTube should be a 'carveout' — does not recommend content based on user interaction or other social connections.
- The potential application of age assurance/verification measures was discussed. Some features of YouTube are disabled if the platform is being used a 'signed out' user experience as there is no way to verify age.
- There was a strong preference for consistency across State and Commonwealth approaches.
- Google uses multiple ways to adhere to the age restrictions, including AI and 'selfie' technology; however, accuracy is limited at this stage of development.

The Age Verification Providers Association

Meeting Date: 14 August 2024

Attendees:

- Mr Iain Corby, Executive Director

Topics Discussed:

- Expert insight regarding the implementation of a defence 'reasonable steps'; how that might look like with respect to current age assurance technologies; the codification of minimum necessary conditions. Ensuring flexibility and amenability to changes.

- The efficacy of age verification and the 'margin of error' for current age assurance and verification technology.

- The practical considerations for the implementation of a third-party age verification provider model.

- The concept of 'Co-regulation' — private sector regulating itself through standards and independent auditors that are assessment bodies approved by the relevant Government authority.

- The effectiveness of age verification technology is highly dependent upon the training data fed to the system. Diversity in training data, particularly in the context of facial age estimation methods.

- Various sources of data dependent on the context, such as licenses, passports, bank records, school records, parental records, could be used to facilitate age verification. Access to Government datasets for age verification methods in the South Australian context.

- The distinction between third-party providers and the utilisation of tokens was discussed. The utilisation of encrypted tokens across social media and online platforms to reduce the constant need to authenticate yourself is being trialled by Mr Corby and his Association at present.

- Caution was given regarding a parental consent model due to the possibility of children merely seeking verification from random adults for these purposes.
- The possibility of designating the responsibility to implement age verification on the device or application provider, for instance, Apple or Google.
- With reference to current online safety regulations in the United Kingdom, the establishment of a level of error which is permissible, perhaps in terms of percentage of targeted individuals who have or have not gained access to a platform.

Snap Inc

Meeting Date: 15 August 2024.

Attendees:

- Mr Henry Turnbull, Head of Public Policy, Asia-Pacific
- Mr Ben Au, Manager, Public Policy, Australia and New Zealand

Topics Discussed:

- Overview of Snapchat's online safety team.
- Snap Inc's Australian subsidiary.
- How Snapchat works — its core functions; Snapchat operates in an environment much more closed that its competitors: primarily a private communication app.
- Snapchat's strict content moderation mechanisms on its content feeds: *Discover* and *Explore.*
- How Snapchat's Family Centre seeks to promote safety for teenagers on the app.
- Age minimum on Snapchat: minimum age of 13 and Snapchat's lack of mechanism to verify the age of users.
- It would be preferable to implement age verification measures at the App Store or device level as opposed to creating a fragmented system where each platform tries to enforce age restrictions in a different way.
- Logistics of how device level verification would work in practice.
- Concern that a ban will just result in children migrating to less regulated and more dangerous platforms.
- Challenge of enforcing a scheme that involves relationships between the States and the Commonwealth.

- Concern of stereotypes that all social media companies are big tech giants will end up unnecessarily harming smaller platforms like Snap Inc, who do not view themselves as a typical social media platform.

TikTok

Meeting Date: 19 August 2024

Attendees:

- Ms Ella Woods-Joyce, Director Public Policy
- Ms Amelia Crawford, Legal Counsel

Topics Discussed:

- TikTok proactively looks at cues and behaviours of their users and if there is a belief the user is underage, they will suspend the account immediately.
- TikTok has an age-appropriate design where the level of content is altered to reflect under 18 or over 18 user.
- There is some concern about holding the identification data when the user is underage and ensuring to only collect the data required to ensure a safe and secure experience.
- Parents can utilise the Family Pairing Tool with the support and approval of their child, which then enables the parent to disable or enable options and settings in the app.
- Concerns with how a territorial link would work if this remained a state model.

Meta

Meeting Date: 19 August 2024.

Attendees:

- Ms Mia Garlick, Regional Director, Policy for Japan, Korea, Aus, NZ and the Pacific.
- Mr Philip Chua, Director of Instagram Public Policy, APAC
- Ms Malina Enlund, Safety Policy Manager, APAC
- Ms Alex Cowen, Policy Programs Manager, Australia
- Ms Bronwyn Lo, Public Policy Manager, Australia

Topics Discussed:

- The competing tension between privacy considerations and the need for personal information to be used for age verification.
- Development of age assurance technologies on Instagram.
- The antagonists are the users themselves: current age verification extremely easy to get around by lying about your age.
- Age verification that relies on personal information for ID has a low success rate and is too easy to avoid, and age verification that relies on facial recognition technology is too often inaccurate to be of much use.
- Meta uses age verification that uses AI to flag users under the age limit based on behaviour on the app, due to the lack of effectiveness of measures at the account creation stage.
- When does age verification need to be implemented: at the device level or at the social media platforms? Age verification at the app store level would prevent fragmented policy trying to apply to every individual app.
- Given the lack of reliability of current age assurance technologies, concerned about Meta's exposure to liability.

- Meta works collaboratively with national regulators, including the eSafety Commissioner.
- Part of the issue is that there are so many different social media applications — children can spend all day jumping from one to the other.
- Whether platforms tailor-designed for children — including YouTube and Messenger Kids, should be exempted from the definition of social media.
- Possibility of enforcement on the global level.

Office for Autism

Meeting date – 21 August 2024

Attendees:

- Ms Maggie Rutjens, A/Director

Topics Discussed:

- There are independent clinical therapeutic approaches to teach independent living skills, social media, cyber hygiene, cyber security, and techniques to assist autistic adolescents to navigate the internet.

- Current existing initiatives in Adelaide include using social media adjacent and gaming platforms for communication and socialising.

- In an online world anxiety and lack of confidence in the autistic person is all but removed as a reliance for immediate reciprocation or processing information is removed.

- Social media is trending towards portraying autism as a more realistic and healthier way than television and film have done in recent years, which is a more accurate and everyday representation of autistic life.

- Apps or social media platforms that have a higher propensity to advertise and influence would have a much higher risk to an autistic person.

Chapter 1: Conclusions and Proposal

The impact of social media

The impact of social media is global. It evolves with new technologies and new applications of existing technology. It provides a variety of means by which people can interact with each other using electronic devices including computers, tablets and iPhones.

Social media can be beneficial, connecting people and their ideas and experiences, providing new and varied means of self-realisation, and providing opportunities for personal and creative self-expression. It can be educative and deliver community support services that may reduce some of the worst effects of social disadvantage including isolation and inequality.

Social media is used for positive support and communication by many elements of the public, private and not-for-profit sectors. The Department of the Premier and Cabinet of South Australia states on its website that it 'uses social media channels to distribute information to the community'.[1] In so doing, it reserves the right to remove various species of incoming content including abusive, harassing or threatening comments, replies or direct messages. The Commonwealth Department of Social Services states on its website that it 'uses a range of social media channels to inform, engage, communicate with and learn from stakeholders.'[2] These examples could be multiplied.

Social media can also be a channel for false and harmful content and a platform for bullying, exploitation and predation. It can be addictive. It can inflict harm on vulnerable members of society and particularly on children. While there are benefits to children learning how to navigate social media and how to use it to advantage there are significant risks. Harms identified by the Office of the eSafety Commissioner, established under the *Online Safety Act*, include:

---

1 Government of South Australia, Department of the Premier and Cabinet, 'Social Media Policy Terms of Use'; https://www.dpc.sa.gov.au/responsibilities/government-communications/social-media-policy-terms-of-use (Accessed 30 August 2024)

2 Australian Government, Department of Social Services, 'Social Media' 13 October 2023 https://www.dss.gov.au/social-media

- Personal safety harms — e.g. direct and indirect threats or facilitation of violence; intimidation and harassment; viral challenges;
- Health and wellbeing harms — self harm and suicide material — material promoting eating disorders and exposure to development mentally inappropriate conduct;
- Harms to dignity — insulting and demeaning comments and trolling;
- Privacy harms including doxing, sexual extortion and image-based abuse;
- Harms involving discrimination, including hate speech, racism, misogyny, sexual harassment, homophobia and transphobia;
- Harms involving perception and manipulation, including grooming of children.

In recognising these harms, it must also be recognised that across the age ranges to 14 years and from 14 to 16, there will be a variety of developmental stages and vulnerabilities — some of which will depend upon the particular circumstances of the individual child. Risk assessments across these age ranges necessarily involve broad generalisations.

The South Australian policy setting

The risks and benefits connected with the use of social media by children are best identified by reference to the investigations and findings of those with expertise and responsibilities in the field. Where a protective regulatory balance should be struck however, is a normative or policy judgment for government informed by evidence and advice.

The Government of the State of South Australia has taken the view that the most appropriate measure is to restrict access by children to social media generally. The Government has also taken the position that between the ages of 14 and 16, access should only be permitted with parental consent or its equivalent. It is against that background that the South Australian Government has commissioned this legal examination of mechanisms for giving effect to its policy setting.

The Terms of Reference state in very broad language the policy setting within which this legal examination is conducted. They refer to the harmful effects on the wellbeing and mental health of children of the use of social media and the shortcomings of existing safeguards which are said not to be in step with community expectations.

The Government acknowledges that the challenges associated with regulating social media services so as to protect children from harm are complex. This independent legal examination has been commissioned by the Premier into 'how to ban children from having social media accounts'. A legislative pathway is proposed which would be within the legislative power of the South Australian Parliament. The Draft Bill is an indicative model of what legislation, to give effect to the Government's policy, might look like. The Draft does not pretend to provide the definitive solution to the challenges of regulation and enforcement in this field — challenges which evolve with the dynamic landscape of social media and social media use.

Existing Commonwealth coverage

Specific online harmful content is the subject of regulatory powers relating to children conferred on the eSafety Commissioner under the *Online Safety Act*. It includes:

- Cyber bullying of children;
- Illegal and restricted online content, including child sexual exploitation material and pro-terror content and pornography;
- Non-consensual sharing of intimate images;
- Material promoting, inciting, instructing in, or depicting abhorrent violent conduct.

The regulatory system presently in place under the Commonwealth legislation does not preclude access to social media by children generally. However, it does have mechanisms in place to prevent access by children to particular classes of content.

The legislative powers of the State of South Australia

It is within the legislative competency of the South Australian Parliament to enact a law imposing State-specific age restrictions on access to social media services. A territorial link to the State is necessary. That requirement is satisfied by the application of the Act to social media services provided or accessible to users within the State and the imposition of the proposed restrictions upon access to children domiciled within the State. As to the relationship with the Commonwealth legislation, the *Online Safety Act* of the Commonwealth expressly allows for the possibility of concurrent State laws. The legislative competency of the State is discussed in a separate chapter of this Report.

The necessary territorial link does pose a practical challenge in that a social media service provider seeking to comply with the restrictions would, as part of that compliance, have to determine which existing and prospective users were domiciled within the State of South Australia. That is a complication which arises from the State-based character of the proposed legislation.

Options for the establishment of a Regulator

As appears from examination of the functions of the Commonwealth eSafety Commissioner, the regulatory task in relation to social media is complex and burdensome. It requires financial and human resources and an accumulation of expertise and experience that cannot be created quickly from a standing start.

It is legally possible for South Australia to create its own bespoke regulator or to confer additional functions on an existing statutory officer such as the Children's Commissioner or the Commissioner for Consumer Affairs. However, a timeline for getting a State Regulator fully functional and operating could be significant. It would be necessary to recruit people with the expertise and experience necessary to administer and enforce the legislation. There would inevitably be some duplication of resources with those provided to the Commonwealth regulator.

An alternative approach would be to secure the agreement of the Commonwealth to confer a new State-based regulatory function upon the Commonwealth eSafety Commissioner. There is precedent for that approach in national regulatory schemes. Examples are:

Section 13A — *Australian Energy Market Act 2004*

Section 6AAA — *Therapeutic Goods Act 1989*

If the State law does not impose any 'duty' on the Commonwealth regulator the consent of the Commonwealth Parliament set out in a law of the Commonwealth would suffice. If the State law purports to confer a duty upon the Commonwealth regulator, that must be a duty which falls within a Commonwealth head of power and is supported by a law of the Commonwealth.

The legislative powers of the Commonwealth supporting its *Online Safety Act* would appear to be sufficient to support a Commonwealth law giving effect to the conferral under State law of

regulatory duties to the eSafety Commissioner in relation to the restriction of access to social media services by children in South Australia.

The choice of regulatory mechanism is a matter for the Government of South Australia and for the Commonwealth if it is decided to try to use the Commonwealth regulator.

Cooperative federal considerations

There is another important federal consideration in any design of a South Australian law. South Australia has taken the initiative in proposing a more protective approach to children's access to social media than presently applies under Commonwealth law. That initiative could itself form the basis for the development of a more comprehensive child protective national scheme than presently exists. It is important that so far as possible South Australian legislation be compatible with the Commonwealth law and capable of providing a template or building block for a cooperative national scheme involving the Commonwealth and other States and Territories of Australia. To that end, the Draft Bill, so far as possible, uses terminology which is consistent with the Commonwealth scheme. A national scheme would remove the requirement for the proposed duty to be limited in its application to children domiciled in South Australia and the compliance and enforcement complications that go with that limitation.

Legislative models in other jurisdictions

Consideration has been given to online safety legislation in other jurisdictions. The European Union, Ireland, the United Kingdom, Canada, the United States and Singapore have been referred to. Consideration has also been given to legislative bans enacted in some States of the United States.

The concepts of:

(1) Exemption of beneficial or very low risk social media services; and

(2) The use of a reasonable steps criterion required for compliance with a duty to provide access,

are derived from some of those examples.

Reflection upon State statutes in the United States has led to the conclusion that their definitions of terms equivalent to 'social media services' are unduly complex, particularly in their lists of statutory exemptions which are likely to give rise to litigious debate.

The model for South Australia

The legislative proposal for South Australia uses a generic definition of 'social media service' based on that which appears in the *Online Safety Act*, but which is broader in order to pick up search engines and App stores. The proposal allows for named social media services or classes of social media service to be exempted from age-based restrictions on access by regulation or ministerial determination. The proposal would impose a duty of care on non-exempt social media service providers to prevent access to their services by minors within the restricted age ranges. It would be a defence to a breach of the duty that the provider had taken reasonable steps to comply with it. A separate systemic duty of care would positively require providers to take reasonable steps to prevent access within the restricted age ranges. The operation of these duties of care is elaborated below.

Regulatory guidelines could set out minimum standards necessary for compliance with the 'reasonable steps' requirements in relation to the duties imposed on providers. The ultimate judgment of whether reasonable steps were being taken would be for a court on an enforcement action. There would, however, be ample room for collaboration between the Regulator, the industry, age assurance providers and other stakeholders to give a degree of certainty in this area which involves the use of age assurance mechanisms and determinations of domicile.

Despite their novelty in the Australian context, the proposed restrictions do not introduce a regulatory approach which is completely unknown to providers. Many major providers already impose a 13-year old age related ban on access. The Commonwealth Act also imposes age-related bans on access to certain classes of material.

Exempt Social media — sifting out the good from the bad and the ugly

The term 'social media service' defined broadly, as in the Draft Bill, has a very wide reach. It encompasses the ugly, the bad and the good. It is important that the child protective approach adopted by South Australia, not throw out the baby with the bathwater. It should allow access to existing and new social media services which are beneficial and very low risk, e.g. dedicated educational services and eHealth services. To that end, the Draft Bill, while precluding access

by children to a widely defined class of social media services, introduces the concept of an 'exempt social media service'. It is proposed that 'exempt social media services' should be listed by name or category determined by the Minister or the Regulator from time to time according to publicly available criteria. The purpose of leaving the question of what is an exempt social media service to be determined by ministerial or regulatory decision is to ensure flexibility in the face of a complex and rapidly changing technological landscape. It is important not to lock definitions into the legislation which would require amendment by Parliament from time to time to cover unanticipated developments. Some of the definitions in the United States State laws are quite elaborate in their lists of exceptions and are not recommended in the legislative model suggested in this Examination.

Duties of care to prevent access

The approach proposed in this Report seeks to give practical and workable effect to the policy of a ban on children's access to social media. In so doing it does not seek to create a hard-edged prohibition supported by a civil penalty regime of first resort. Rather, it seeks to implement the policy by creating two statutory duties of care. The primary duty would be a duty on a social media service provider to prevent access to its social media service in South Australia by any child under the age of 14 and by any child between the ages of 14 and 16 without the consent of their parents or a person in place of their parents. The second duty would be a duty on a social media service provider to take all reasonable steps to prevent access to their social media service by any person under the age of 14 and by any person between the ages of 14 and 16 without parental consent. These are not just duties to protect children against unsafe online content. They are more comprehensive than the duties of care provided in some other jurisdictions. These are duties of care directed to prevent children from having access to non-exempt social media at all in the lower age range or without parental consent if within the higher age range. Branding them as' duties of care' rather than as a general prohibition emphasises the purpose of the legislation which is to give effect to a policy protective of children. The children to whom the duties would apply would be children domiciled or resident in South Australia. The verification of domicile would raise an additional challenge for social media service providers and for the Regulator under the South Australian law. It would be necessary to exclude the application of the duty to children from other States or countries

visiting South Australia, e.g., for holiday purposes. A diagram showing a possible decision tree for a provider complying with the duty is attached to this chapter.

A reasonable steps requirement

The proposed duties are technologically agnostic. They do not specify the means which a provider must adopt in determining whether access to a user is to be permitted or denied. Plainly, compliance will require the use of age verification and estimation mechanisms. But the means currently available for verification and estimation are still in development.[3] The hard fact is that there is no error free means of determination of the age of users of an account.

There is also a complication in terms of compliance where, as in this case, the relevant duties apply only in relation to children living in South Australia. To know whether the duties apply to it, a social media service provider must know where the proposed user lives. Again that verification — as to address or a location within the State would have to be subject to a 'reasonable steps' standard.

In order to encourage providers into a cooperative rather than adversarial stance with the regulator, it should be open to them to demonstrate, on an allegation of a breach of the first duty, that they have taken all reasonable steps, having regard to available technology, to discharge that duty. The second duty, supportive of the first and directly imposing the reasonable steps requirement, provides the means for a proactive enforcement regime and the development of regulatory guidance as to what constitutes reasonable steps to comply with the restricted access duty. Ongoing consultation with providers and other stakeholders would be essential.

Modes of enforcement — individual complaints and regulatory inspection

The proposed Act would provide different ways in which the duties of care are to be enforced. The first way, relevant to the primary duty, would be likely, for the most part, to depend upon complaints made to the regulator. It would arise where a child under the age of 14 is given access to the provider's social media service, or where a child between the ages of 14 and 16 is given such access without parental consent. There is a limitation to this enforcement mechanism. Complaints-based enforcement is ad hoc and reactive. It would depend in many

[3] eSafety Commissioner, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography', March 2023.

cases upon a parent becoming aware of a child's use of a non-exempt social media service and reporting that use to the regulator. The problem with such a complaint-based process, apart from its ad hoc and reactive character, is that it may involve the child in enforcement proceedings. On the other hand, it would be open to the State to treat a breach of the primary duty as a statutory tort, actionable in damages where a child has suffered significant mental or physical harm as a result of the breach. The action could be taken by the child through a legal representative or perhaps by the Regulator on behalf of the child.

As to the second duty, the question whether a provider has taken reasonable steps to prevent access or access without parental consent could be explored by a process of information gathering from the provider by the Regulator, supported by coercive request powers. Such requests could require the provision of information by a provider relating to its system for verification of domicile, age verification and verification of parental consent where applicable. The Regulator could issue guidance from time to time, of what would constitute reasonable steps. Alternatively, minimum measures necessary to meet the reasonable steps requirement could be specified in a legislative instrument without thereby pre-empting a determination whether they are sufficient in a particular case to meet that requirement.

Sanctions

Sanctions for non-compliance with either duty of care, could include the following:

(1) The issue of a remedial notice to the provider to institute a process for age, domicile and parental consent verification that meets the threshold of reasonable steps.

(2) An enforceable undertaking.

(3) An infringement notice imposing a specified compensation payment to be made which is capable of challenge in the court. The compensation payment would be applied to a special fund of the kind referred to below.

(4) The institution of proceedings in court for the imposition of all or any of the following remedies:

    (i) a declaratory order;

    (ii) injunctive relief and/or corrective orders;

(iii) a compensation order;

(iv) a civil penalty.

A compensation order would not have the character of a civil penalty. Its proceeds could be paid into a fund to promote research into and education about the effects of social media on children and the means of developing beneficial social media services for children. It could also provide for the discretionary payment of compensation, upon application, for the benefit of a child shown to have suffered harm as a result of exposure to a non-exempt social media service.

(5) It would be appropriate to seek a civil penalty where there has been wilful or reckless or repeated breaches of one of the duties, non-compliance with a statutory requirement for the provision of information or breach of an enforceable undertaking or an injunction. The amount of the civil penalty could be fixed by regulation.

(6) A breach of the first duty of care could also constitute a statutory tort where mental harm has resulted. Proceedings for damages for breach of the statutory duty in such a case could be taken by a legal representative of the child harmed or by the Regulator on behalf of the child.

Ongoing policy development

A point of importance was made by the Chief Psychiatrist of South Australia about the need for ongoing proactive development of a knowledge base and policies to respond to the harms of social media services and to encourage the development of beneficial social media services or protected uses of existing social media services. An example of a protected use was given by Department for Education officers who spoke of teachers in South Australian schools using Facebook with their students where the Facebook account was controlled by the teacher and was not an account accessible by the students.

The US Surgeon-General in an Advisory Statement about Social Media and Youth Mental Health, which was issued in 2023, observed that researchers would play a critical role in helping to gain a better understanding of the full impact of social media on mental health and wellbeing and informing policy, best practices and effective interventions. A means by which research could contribute included:

- rigorous evaluation of social media's impact;
- the role of age, developmental stage, cohort processes and the in-person environment;
- benefits and risks associated with specific social media designs, features and content;
- long term effects on adults with social media use during childhood and adolescence;
- the development and establishment of standardised definitions and measures for social media and mental health outcomes;
- the development and establishment of standardised definitions and measures for social media and mental health outcomes;
- evaluation of best practices for healthy social media use;
- enhancement of research coordination and collaboration.

A statutory mechanism already in place in South Australia which might be able to take on the oversight of research, policy development and collaboration incidental to the statutory regime, is the Child Development Council, established under s 46 of the *Children and Young People (Oversight and Advocacy Bodies) Act 2016* (SA). Although its primary function under s 55 of that Act is to prepare and maintain the Outcomes Framework for Children and Young People, it has additional functions which include advising and reporting to government on the effectiveness of the Outcomes Framework for Children and Young People for which the Act provides. It may also carry out:

> such other functions as may be assigned to the Council under this or any other Act or by the Minister.[4]

This would enable the Council to be given what would amount to policy development functions for the purposes of the further development of policy in relation to restriction of access to social media services and the development of exempt social media services. The Council already has a duty under s 55(3) in performing its functions to seek to work collaboratively with:

(a) State authorities and Commonwealth agencies that have functions that are relevant to those of the Council; and

[4] *Children and Young People (Oversight and Advocacy Bodies) Act 2016* (SA), s 55(2)(c).

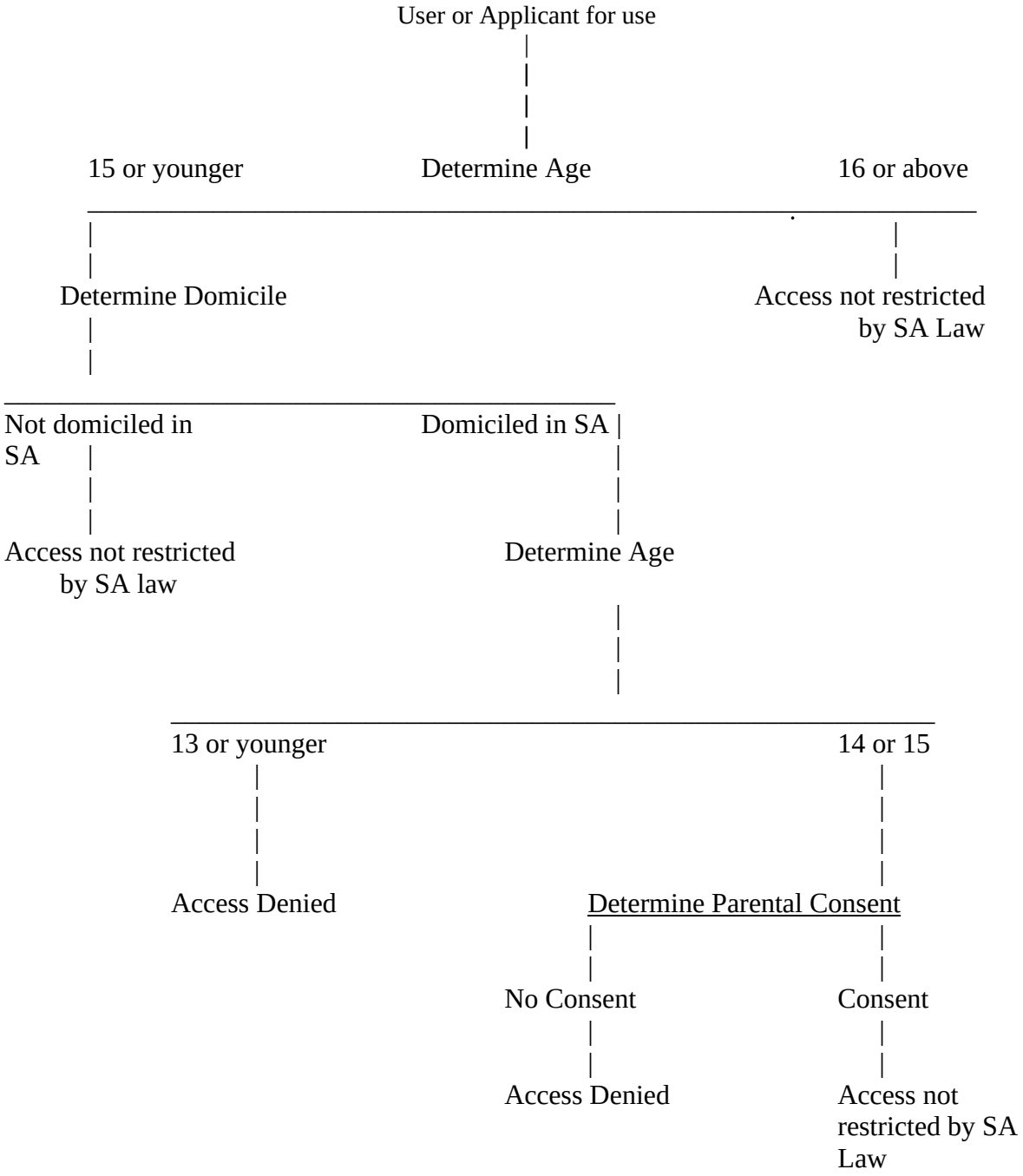
(b) Relevant industry, professional and community groups and organisations.

This could include engagement with providers in what might be a more flexible, high-level way than would be prudent for the regulator to undertake. Alternatively, some other body or authority may be established for that purpose.

Conclusion — not a counsel of perfection

Whatever regime is established by the South Australian Government, it will not be perfect. Effecting compliance across the industry will be challenging. Compliance will require age assurance measures, location measures and, where applicable, verification of parental consent. Enforcement measures may be complicated by the fact that many providers are companies which are located outside Australia. The legislation would apply to existing as well as prospective users of social media services. There will undoubtedly be workarounds by knowledgeable child users. However, the perfect should not be the enemy of the good. One non-legal beneficial effect of the law may be to arm parents with the proposition that it is the law not them that restricts access to social media for children in South Australia.

Decision Tree



Chapter 2: Children's usage of social media and its risks and benefits

Introduction

In the consultations in aid of this legal examination, there was a general view that there are both risks and benefits associated with access to the internet by children in the age ranges of interest. There were however differences about the weight to be accorded to those risks and benefits and whether a 'ban' would be good policy.

Some of those consulted were of the opinion that a general ban on access to social media was not in the interests of children. As a broad generalisation they should be protected from unsafe content and predators, but also helped to learn to navigate social media and to use it as an aid for their own education and development. Others thought that the risks to safety and personal development were such that nothing less than a general restriction on access would suffice.

There has been debate in the public domain about the balance between risks and benefits for children and young people under the age of 16 arising from engagement with social media services. This Report does not offer a detailed and granular account of that debate, but refers to some sources to identify its salient features. They were of assistance in aiding an understanding of the complexities of this area of social policy. That understanding also indicates the need for a nuanced legislative response to the extent that it is compatible with the underlying policy of the government.

Before turning to materials considered in the examination for a greater understanding of identified risks and benefits, it is useful to refer to the current extent of social media usage by children in Australia.

Social media usage by children in Australia

Usage by children and young people aged 8 to 17 years

Young people use social media platforms differently to adults. For young people, these platforms are the infrastructure of everyday life. They take them for granted as the routine means to sustain relationships, express identities, and build networks (Office of the eSafety Commissioner, 2022, p. 33).

Research by the Office of the eSafety Commissioner (2018)[5] found the top five social media services used by young people aged 8 to 17 years (children aged 8 to 12 years, teenagers aged 13 to 17 years) at the time were:

- YouTube: 80% children, 86% teenagers
- Facebook: 26% children, 75% teenagers
- Snapchat: 26% children, 67% teenagers
- Instagram: 24% children, 70% teenagers
- Google+: 23% children, 29% teenagers

Gender differences

The same research identified some gender differences between the types of social media used by children and young people aged 8 to 17 years in Australia.

In 2017, girls were more likely to use:

- Instagram: 52% girls, 42% boys
- Snapchat: 53% girls, 39% boys
- Pinterest: 23% girls, 8% boys
- Musical.ly: 18% girls, 6% boys
- Tumblr: 12% girls, 4% boys

And, boys were more likely to use:

- YouTube: 85% boys, 81% girls
- Reddit: 8% boys, 4% girls

[5] Office of the eSafety Commissioner, 'State of Play-Youth, Kids and Digital Dangers' (2018). https://www.esafety.gov.au/research/youth-digital-dangers

Number of social media services used, and duration of use — eSafety Commissioner (2021)

In 2021, the Office of the eSafety Commissioner examined the online behaviours and experiences of young Australians.[6] The results indicated that teenagers (aged 12 to 17 years):

- spent an average of 14.4 hours per week online (just over two hours a day), and males spent more time online (15 hours), compared to females (13.8 hours), for a range of activities, including:
    - researching topics of interest – 95%
    - watching videos, movies or TV – 93%
    - chatting with friends – 93%
    - listening to music – 92%
    - online gaming – 77%
- used an average of four different social media services, with the average number increasing with age: 12 to 13 year olds used an average of 3.1 services, compared with 4.5 for those aged 16 to 17.
- in older age groups (14 to 17 years) were more likely to use social media services, with 12 to 13 year-olds using an average of 3.1 services compared with 4.5 for 14 to 17 year-olds.
    - *Note that, for many social media services, the minimum age for social media accounts is 13, suggesting that some 12 year-olds may not be providing accurate age information in their profiles.*
- most commonly used the following social media services:
    - YouTube – 72% (compared to 86% in 2017)

6 Office of the eSafety Commissioner, 'The digital lives of Aussie teens' (2021) https://www.esafety.gov.au/sites/default/files/2021_02/The%20digital%20lives%20of%20Aussie%20teens.pdf

- Instagram – 57% (66% in 2017)
- Facebook – 52% (66% in 2017)
- Snapchat – 45% (63% in 2017)
- TikTok (formerly known as Musical.ly) – 38% (12% in 2017)
- Discord, established in 2015, was used by 19% of Australian teens in 2020.

Usage of social media services — Commissioner for Children and Young People

The South Australian Commissioner for Children and Young People provided a helpful account of current use of apps and social media by young people. Speaking qualitatively, she reported that young people use social media to connect with people and community. They follow:

- Friends, family and other people they know offline, both those who live interstate or overseas as well as those who live locally.
- People who inspire, entertain or help them relax, including sports teams, artists, musicians, actors, authors, leaders, activists, influences or role models, comedians or animals;
- People and communities across the world with similar interests including fandoms, movies, musicians or artists.

Young people were said to use social media to pursue a wide range of interests and learn new things. They seek information about what is happening around them in order to support their school work as well as their aspirations for study, work and travel in the future. By way of example the Commissioner stated that they follow:

- Video essayists on YouTube to learn more about a wide range of interests, including pop culture, history, science, engineering or art;
- News or journalism accounts to keep up to date with political events;
- Travel blogs and 'young backpackers on gap years' to see different parts of the world and get travel tips and inspiration;

- Local businesses and organisations to learn about ‘events in my home town’ and opportunities available to them;
- ‘Foodie’ accounts to find and share recipes and seek recommendations;
- Tutorials to learn dances, makeup and fashion or styling trends;
- Local or global artists, coders or gamers who inspire their own art, music, videos, dance, gaming, coding;
- Accounts related to nutrition, gym or fitness to support physical activity.

The most popular platforms overall were said to be:

- Instagram, Snapchat, TikTok, Discord and YouTube. Other platforms which were mentioned include X (formerly Twitter), Pinterest, Tumblr, Reddit and Steam.

Snapchat and Instagram were the most common platforms which young people use to chat, followed by Message apps (texting apps on iPhone or Android), Discord, WhatsApp and Messenger. Most used Message apps to chat with family and Snapchat and Instagram to chat with friends. A few used Telegram and Skype to chat, but this was less common.

Instagram and TikTok were the most common platforms for creating and sharing content, followed by YouTube and Snapchat. Some also used Adobe designed software, video editing software or Tumblr to create content. Messaging apps, Facebook, Tumblr, Reddit and X, were also used for sharing content.

Instagram and Snapchat were the most common platforms used to see what friends are doing, followed by TikTok, Discord and Messaging Apps. Pinterest was also mentioned.

Instagram and TikTok were the most common platforms used by young people to find out news, followed by Google apps or websites. Others mentioned Facebook, YouTube, X, the ABC, other news apps or newspapers.

Roblox, Steam and Discord were the most common platforms used by young people for gaming. Discord was also used to chat (voice, video and text) with others while gaming. Minecraft was also popular. Some young people mentioned apps or websites for puzzles, chess,

sudoku or language/learning (Duolingo) while others mentioned consoles such as Xbox or PlayStation, specific games or game companies and developers.

It should be noted that the young people referred to by the Commissioner appear to have been young people in Years 10 to 12 who are members of her South Australian Student Representative Council.

Reported negative online experiences — eSafety Commissioner (2021)

In the six months prior to September 2020, four in 10 teenagers (44%) had a negative online experience (Office of the eSafety Commissioner, 2021). *Note: While detailed comparisons with 2017 data was not possible due to different survey methodologies, the type of negative online experiences reported by young people in 2020 and 2017 are broadly consistent.*

In 2020, the top three negative experiences for teenagers online were:

- being contacted by a stranger or someone they didn't know (30%)
- being sent unwanted inappropriate content such as pornography or violent content (20%), and
- being deliberately excluded from events/social groups (16%).

As shown in Table 1 below (excerpt from Office of the eSafety Commissioner, 2021), the likelihood of having a negative online experience increased with age and was greater for young females:

- 47% of females had a negative online experience compared with 41% of males
- females were more likely to be contacted by a stranger (35% compared with 26% of males), and
- males were slightly more likely to receive online threats or abuse (18% compared with 11% of females).

Table 1: Negative online experience in the six months to September 2020, by gender and age

	Total	Gender		Age (years)	
		Male	Female	12 to 13	14 to 17
I was contacted by a stranger/someone I didn't know	30	26	35	19	36
I was sent inappropriate unwanted content*	20	20	20	13	23
I have had other negative experiences online in the past six months	16	14	18	14	17
I was deliberately excluded from events/social groups	16	16	17	11	19
Things were said about me to damage my reputation	15	16	13	12	16
I received online threats or abuse	15	18	11	14	15
Someone misused my personal information/photos online in a mean way	8	9	6	5	9
At least one negative online experience	**44**	**41**	**47**	**32**	**51**
Base (number)	627	313	314	191	436

Q3: Have you experienced any of the of the following [negative online experiences] in the past 6 months? *e.g. pornography or violent content.

Reported positive online experiences

In its submission to the Inquiry into Social Media and Online Safety, the Office of the eSafety Commissioner (2022, p. 32) identified several positive effects of social media use by young people on their wellbeing, including:

- building and strengthening relationships
- peer support and immediate relief from the emotional load from people with shared experiences
- bolstering formal education (e.g. through forums, discussion boards, blogs or video tutorials) and informal education (e.g. through news or DIY videos)
- providing a safe place to find support and legitimisation for their identities (e.g. cultural, sexual, ethnic), and experiences (e.g. illness, disability)
- and allowing lonely young people to feel less shy by chatting online and feeling they belong to a group.

There have been a number of publications and public statements from a variety of sources concerning both risks and benefits.

The Royal Australian and New Zealand College of Psychiatrists' Position Paper — 2018

In 2018 the Royal Australian and New Zealand College of Psychiatrists issued a Position Paper on the impact of media and digital technologies on children. The Report identified positive benefits of media and digital technologies for children and also raised areas of concern. The Position Paper included, but was not limited to, social media.

General benefits of media and digital technology listed were as follows:

- Social media sites provide young people with opportunities to connect with friends and family and develop technical and creative skills. They facilitate connection to a diverse and widespread group of people providing a greater understanding of global issues.
- There is evidence that media can have positive effects on social skills in children, and that experiences of using social media platforms are generally positive.
- Education can be enhanced in a number of ways through various media interfaces allowing students to engage in self-directed learning, collaboration on group projects and the exchange of ideas about homework. Engagement with digital delivery of material allows children and young people to enhance and consolidate learning on an almost inexhaustible range of topics.
- Electronic games and devices can be used to increase physical activity in children and, with the development of technology, allow for outdoor games and activity.

Examples of e-health related benefits were as follows:

- Technology provides information about a range of physical and psychological health problems of relevance to young people, which may lead to a positive benefit in terms of promoting engagement with health-care services. An increasing number of apps are designed for children and adolescents and to encourage behaviours such as healthy activity, enhanced medication adherence and smoking cessation, as well as specific mental health benefit.
- Mental health promotion, including to promote resilience, support parenting and family mental health, address risk factors for mental health problems and disorders, and increase mental health literacy.

- A growing body of evidence supports the effectiveness of e-health interventions for a number of mental health problems which can be provided in a timely manner, in privacy and at the individual's discretion. E-health intervention may be used to increase access to treatment in remote and rural areas where distance and workforce shortages are a challenge. The World Psychiatric Association has developed a position statement on e-mental health which may help psychiatrists provide guidance in this area.

- The lives of children and young people accessing media technology who have taken advantage of opportunities such as these could be enriched.

The College also identified what it called the 'problematic impact of media' as follows:

- *Problem internet use* ('PIU')— there is no internationally agreed definition on what constitutes PIU however a sensible working definition was put forward as:

  > the pervasive long term and heavy use by a person of internet and computer-based technologies, including gaming, that is out of keeping with one's educational, social or occupational role, wellbeing and health.[7]

  Some consider that in its most severe form, PIU can be considered an addictive condition (internet addiction), showing features such as dependence, mood alteration, tolerance, withdrawal and harm to psychosocial functioning. It is increasingly recognised as having a potentially significant impact on mental health to varying degrees.

- *High use of social media* — a survey by the Australian Psychological Association in 2017 was referred to. It had found that adolescents spent 3.3 hours a day on social media with some logging on as much as 50 times per day. High use of social media and technology impacted self-esteem, with two in three adolescents feeling pressure to look good. Many are contacted by or make contact with strangers via Facebook, with 15% of respondents in the survey saying this occurs daily. The impact of social media on the mental health and well-being of young people is largely unknown. Encouragement of better patterns of use may help to minimise harmful effects.

---

[7] The Royal Australian & New Zealand College of Psychiatrists, 'The Impact of media and digital technology on children and adolescents', May 2018 citing P Tam, 'Virtual addiction: A 21st century affliction' *Finance Matters* Summer: 6 (2011).

- *Cyberbullying and sexting* — bullying was said to a major problem in Australia and New Zealand. Cyberbullying was defined as 'deliberately using digital media to communicate false, embarrassing or hostile information about another person.'[8] The potential for those who engage in bullying at a distance from their victims means that those affected have limited places and times when they do not feel under threat. There was evidence of a consistent relationship between cyberbullying and depression and some association with other mental health problems. There have been accounts of suicide associated with cyberbullying.

  Sexting is the sending of provocative or sexual photos, messages or videos. They are generally sent using a mobile phone, but can include posting material online.

- *Privacy* — Many online activities, such as subscribing to content, entering competitions and playing online games, require users to enter personal information. The information may then be misused by others, including spam, scams, identity theft and fraud. Young people are also specifically targeted by advertisers who may sell their personal information to other organisations/marketers.

- *Aggression* — There continues to be controversy about the extent to which exposure to media violence causes aggression. Impacts are likely to be different at different ages and effects will be mediated by other influences to which a child or young person is exposed. The extent to which exposure to violence encourages aggression and minimises the impact of aggression — especially when played out in a fantasy world — remains a particular issue.

- *Sexualisation* — The sexualisation of children refers to the imposition of adult models of sexual behaviour and sexuality onto children and adolescents at developmentally inappropriate stages and in opposition to the healthy development of sexuality. The use of sexualised images may occur in popular media. A virtually limitless store of pornography on the internet means that children and adolescents have easier access to more varied, explicit and sometimes violent, unsafe and non-consensual sexual content. Exposure is highly likely to occur. The Position Paper referred to an Australian Institute of Family Studies Report which found that just under half of children aged 9-16 had

[8] The Royal Australian & New Zealand College of Psychiatrists, 'The Impact of media and digital technology on children and adolescents', May 2018 citing GS O'Keefe and K Clarke-Pearson, 'The Impact of social media on children, adolescents and families,' (2011) *Paediatrics* 127:800–4.

encountered sexual images in the past month and that this exposure to mainstream, online pornography could have a range of negative effects.

American Academy of Paediatrics — 2018

A technical report was published by the American Academy of Paediatrics in 2018 under the heading 'Children and Adolescents and Digital Media'. The abstract observed that evidence suggested that the newer interactive and social media offer both benefits and risks to the health of children and teenagers. Benefits identified included early learning, exposure to new ideas and knowledge, increased opportunities for social contact and support and new opportunities to access health advice and information. The risks of such media were said to include negative health effects on sleep, attention and learning, a higher incidence of obesity and depression, exposure to inaccurate, inappropriate or unsafe content and contacts and compromised privacy and confidentiality. The technical report undertook a literature review in relation to those opportunities and risks. The review was framed around clinical questions for children from birth to adulthood. It was suggested that a healthy Family Media Use Plan individualised for a specific child, teenager or family could identify an appropriate balance between screen time/online time and other activities, set boundaries for accessing content, guide displays of personal information, encourage age-appropriate critical thinking and digital literacy and support open family communication and implementation of consistent rules about media use.[9]

International Journal of Environmental Research and Public Health — 2022

An extensive literature review on risks identified and discussed in published articles was published in the *International Journal of Environmental Research and Public Health.*[10] The research was designated as a Scoping Review and was conducted by the Italian Paediatric Society Scientific Communication Group. Its stated aim was to review international literature on social media, their effect and the identification of risks correlated to social media use by children and adolescents. The Scoping Review covered 68 publications, of which 19 dealt with depression, 15 with diet, and 15 with psychological problems which appeared to be the most reported risk of social media use. Other identified associated problems were sleep, addiction,

[9] American Academy of Paediatrics, Children, Adolescents and Digital Media, Technical Report published in (2016) 138 *Paediatric*s.

[10] 2022, August 19 (16): 9960.

anxiety, sex related issues, behavioural problems, body image, physical activity, online grooming, sight, headache and dental caries. The authors in their abstract stated:

> Public and medical awareness must rise over this topic and new prevention measures must be found, starting with health practitioners, care givers and websites/application developers. Paediatricians should be aware of the risks associated to a problematic social media use for the young's health and identify sentinel signs in children as well as prevent negative outcomes in accordance with the family.

eSafety Commissioner's Submission to Inquiry into Social Media and Online Safety — January 2022 — Positive effects

In January 2022, the Office of the eSafety Commissioner made a submission to the Inquiry into Social Media and Online Safety. The submission observed that there are acknowledged benefits of social media for young people, including building and strengthening relationships, peer support and immediate relief from the emotional load from people with shared experiences; bolstering formal and informal education and providing a safe place to find support and legitimisation for their identifies and experiences. It could also have the effect of allowing lonely young people to feel less shy by chatting online and feeling they belonged to a group. Reference was made to expert witnesses before the Inquiry who had also articulated those positive effects. The Commissioner also stated that the online world provided crucial help-seeking avenues for those experiencing distress, including eSafety's own reporting scheme. Youth mental health and support services had increasingly used social media platforms to raise awareness of their services and connect with young people through the medium in which they most actively participate. Mental health services, meeting children and young people where they are, were overcoming barriers to help seeking and could provide self-help content young people could save for future reference and share with their peers. Such services allowed for deeper engagement with young people. Examples were given which were said to show that social media and online peer-to-peer connections could have a positive effect on people experiencing mental ill-health, advancing efforts to promote mental and physical wellbeing. [11]

US Surgeon-General's Advisory Social Media and Youth Mental Health issued in 2023

The Surgeon-General called attention to growing concerns about the effects of social media on youth mental health. His advisory described current evidence on the positive and negative impacts of social media on children and adolescents. In opening the Advisory he observed that

---

[11] eSafety Commissioner, Submission No 53 to *Inquiry into Social Media and Online Safety'*, (January 2022) 32-33.

social media use by youth is nearly universal. Up to 95% of youth in the age ranges 13 to 17 report using a social media platform, with more than a third saying they use social media 'almost constantly'. And although age 13 is the commonly required minimum age used by social media platforms in the US, nearly 40% of children aged 8 to 12 years use social media. Robust independent safety analyses on the impact of social media on youth had not yet been conducted. However, there were increasing concerns among researchers, parents and care givers, young people, health care experts and others about the impact of social media on youth mental health.

The Advisory set out both potential benefits and potential harms of social media use among children and adolescents.

The acknowledged benefits were provision of positive community and connection with others who share identifies, abilities and interests. Social media can provide access for young people to important information and create space for self-expression. Positive effects of social media use for youth include the ability to form and maintain friendships online and develop social connections. It can afford opportunities for positive interactions with more diverse peer groups than are available offline and could provide important social support to youth. It can also provide buffering effects against stress for those who are often marginalised, including racial, ethnic and sexual and gender minorities. A majority of adolescents were said to have reported that social media helped them feel more accepted (56%), that they have people who can support them through tough times (67%) and that they have a space to show their creative side (71%). Further they were more connected to what was going on in their friends' lives (80%). The research also suggested that social media based and other digitally based mental health intervention could be helpful for some children and adolescents by promoting help-seeking behaviours and serving as a gateway to initiating mental health care.

As to potential harms, the Advisory referred to a longitudinal cohort study of US adolescents aged 12 to 15 years (6,595 in total) that found that adolescents who spent more than three hours per day on social media faced twice the risk of experiencing poor mental health outcomes including symptoms of depression and anxiety.

Eighth and tenth graders as of 2021 were said to spend an average of 3.5 hours per day on social media. Reference was made to what was called a 'unique natural experiment' that leveraged the staggered introduction of a social media platform across US colleges. The rollout

of the platform was said to have been associated with an increase in depression (9% over baseline) and anxiety (12% over baseline) among college aged youth, across a total of 359,827 observations. Further, correlational research on associations between social media use and mental health had indicated reason for concern and further investigation. The studies pointed to a higher relative concern of harm in adolescent girls and those already experiencing poor mental health, as well as for particular health outcomes like cyber-bullying related depression, body image and disordered eating behaviours and poor sleep quality linked to social media use. Reference was made to a study conducted among 10,904 14 year olds which found that greater social media use predicted poor sleep, online harassment, poor body image, low self-esteem and higher depressive symptoms cause with a larger association for girls than boys. Primary matters for concern were harmful content exposure and excessive and problematic social media use.

The Advisory acknowledged that the relationship between social media and youth mental health is complex and potentially bi-directional. Lack of access to data and lack of transparency from technology companies had been barriers to understanding the full scope and scale of the impact of social media on mental health and wellbeing. Critical areas of research have been proposed to fill knowledge gaps and create evidence-based interventions, resources and tools to support youth mental health.

Options open to policy makers were said to include:

- the strengthening of protections to ensure greater safety for children interacting with all social media platforms;
- the development of age appropriate health and safety standards for technology platforms;
- requiring a higher standard of data privacy for children;
- pursuing policies that further limit access in ways that minimise the risk of harm to social media for all children, including strengthening and enforcing age minimums;
- ensuring that technology companies shared data relevant for the health impact of their platforms;

- support for development, implementation and evaluation of digital and media literacy curricula in schools and within academic standards;
- support increased funding for future research;
- engage with international partners.

The risks of children's interaction with social media

As appears from the above there is ample evidence to show that while there are benefits to children's interaction with social media, it is also linked to children and young people experiencing harm.[12] Children are widely recognised as amongst the most at-risk groups in relation to online harm.[13]

Risks connected with children's interaction with social media include exposure to inappropriate content (for example, pornography), exposure of personal information (for example, images, date of birth, or details that can be used to triangulate the child's physical location), and cyberbullying.[14]

Evidence provided to the Select Committee on Social Media and Online Safety in 2022 indicated that children interacting with social media were also at risk of:

- being targeted or 'groomed' by perpetrators as part of the production and distribution of child sexual abuse material;
- exposure to illegal or disturbing content, such as violent or abhorrent content, or material promoting harmful or dangerous behaviours (e.g. acts of violence, suicide ideation, promotion of eating disorders),

---

12 U.S Surgeon General's Advisory, *Social Media and Youth Mental Health*. Published 2023. Available at: https://www.ncbi.nlm.nih.gov/books/NBK594761/pdf/Bookshelf_NBK594761.pdf. (Accessed 12 June 2024.)

13 Commonwealth of Australia, *Social Media and Online Safety: Report of the Select Committee on Social Media and Online Safety*, Published 2022, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report/section?id=committees%2freportrep%2f024877%2f78951#footnote5target (Accessed 5 June 2024).

14 Bozzola et al, *The use of social media in children and adolescents: scoping review on the potential risks*, International Journal of Environmental Research and Public Health, 19(16), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9407706/ (Accessed 11 June 2024.)

- discrimination (on the basis of sex, gender, sexual orientation, ethnic background, religious belief, political views, and others,
- technology-facilitated abuse (including the non-consensual distribution of explicit images, deep-fake or cheap-fake image abuse, cyber-flashing, utilising tracking devices or software to monitor a person without consent, and controlling access to accounts or technology).
- Identity theft or imitation, including people using fake social media accounts of others. [15]

The eSafety Commissioner's typology of online harm — 2022

The Office of the eSafety Commissioner has developed a typology of online harm[16] to categorise online harms from a human rights-based perspective. These include:

- personal safety harms – for example, direct and indirect threats or facilitation of violence; intimidation and harassment; viral challenges,
- health and wellbeing harms – for example, self-harm and suicide material; material that promotes eating disorders; children's exposure to developmentally inappropriate content,
- harms to dignity – for example, insulting and demeaning comments; trolling to provoke and disturb other users,
- privacy harms – for example, doxing; sexual extortion; image-based abuse
- harms involving discrimination – for example, hate speech; racism; misogyny; sexual harassment; homophobia and transphobia, and

---

15 Commonwealth of Australia, *Social Media and Online Safety: Report of the Select Committee on Social Media and Online Safety*, Published 2022, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report/section?id=committees%2freportrep%2f024877%2f78951#footnote5target (Accessed 5 June 2024).

16 eSafety Commissioner, Submission No 53 to *Inquiry into Social Media and Online Safety*. (January 2022) Available at: https://www.esafety.gov.au/sites/default/files/2023-04/eSafety-submission-Inquiry-into-social-media-and-online-safety.pdf (Accessed 5 June 2024).

harms involving deception and manipulation – for example, mis/disinformation; scams; catfishing; recruitment to extremism; grooming of children.

The Office of the eSafety Commissioner[17] has also described the roles of content production, distribution and consumption in relation to harm:

- the production of content – for example, where a perpetrator makes contact with a victim in an attempt to groom, coerce or force them into the production of content, or where coerced sexual activity or abuse is recorded,
- the distribution of content – for example, where abusive material is posted, reshared or live-streamed online, which can compound the trauma experienced by victims harmed in the production of content, and
- the consumption of content – for example, where a person's behaviour, emotions, mental health, attitudes or perceptions are negatively impacted as a result of access or exposure to harmful content.

Online harms defined by the Online Safety Act 2021

The *Online Safety Act 2021* defines the specific types of online harm that the eSafety Commissioner regulates through its complaints and removal schemes. They include:

- cyberbullying of children,
- illegal and restricted online content ('class 1' material includes child sexual exploitation material and pro-terror content; 'class 2' material includes material that may be unsuitable for children, such as pornography),
- non-consensual sharing of intimate images,
- adult cyber abuse, and
- material which promotes, incites, instructs in or depicts abhorrent violent conduct.

[17] eSafety Commissioner, Submission No 53 *to the Inquiry into Social Media and Online Safety* (January 2022).

Cyber-bullying of children

The meaning of 'cyber-bullying material targeted at an Australian child' is given by s 6 of the *Online Safety Act* which in the key parts of the definition provides:

> **6 Cyber-bullying material targeted at an Australian child**
>
> (1) For the purposes of this Act, if material satisfies the following conditions:
>
> (a) the material is provided on:
>
> (i) a social media service; or
>
> (ii) a relevant electronic service; or
>
> (iii) a designated internet service;
>
> (b) an ordinary reasonable person would conclude that:
>
> (i) it is likely that the material was intended to have an effect on a particular Australian child; and
>
> (ii) the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child;
>
> (c) such other conditions (if any) as are set out in the legislative rules;
>
> then:
>
> (d) the material is ***cyber-bullying material targeted at the Australian child***; and
>
> (e) the Australian child is the ***target*** of the material.

Research by the Office of the eSafety Commissioner over the years has indicated that cyberbullying of children is relatively common and has been for some time. In her submission to the Inquiry into Social Media and Online Safety in 2022, the eSafety Commissioner reported that:

- one in five Australian young people reporting being socially excluded, threatened or abused online in the 12 months prior to June 2017[18]

[18] eSafety Commissioner Submission No 53 to the *Inquiry into Social Media and Online Safety* (January 2022).

- one in five Australian young people (15% of children (aged 8–12 years), 24% of teenagers (aged 13–17 years)) admitted to behaving in a negative way to a peer online – such as calling them names, deliberately excluding them or spreading lies or rumours. Of these, more than 90% had had a negative online experience themselves.[19]

In a Safety by Design Overview, published in 2019, the Office of the eSafety Commissioner[20] reported that it had received over 1,000 complaints about cyberbullying affecting Australian children. An analysis of the reports by the Office found that:

> The most common complaints include nasty comments and serious name calling (including those that incite suicide and self-harm), impersonation or hacking of social media accounts, unwanted contact, sexting and image-based abuse. Our experience shows that children and young people are predominantly bullied online by those in their own peer group. In many instances, cyberbullying is an extension of bullying or conflict occurring within the school. In reports to eSafety, victims often note that the harassment they experience online broadly mirrors their experience at school. Further, the perpetrators are, in many instances, one and the same.[21]

Illegal and restricted content online

The term 'illegal and restricted online content' refers to, '…content that ranges from the most seriously harmful material such as images and videos showing the sexual abuse of children or acts of terrorism, through to content that should not be accessed by children, such as simulated sexual activity, detailed nudity or high impact violence'.[22]

The *Online Safety Act* defines illegal and restricted online content as either 'class 1 material' or 'class 2 material', which is assessed with reference to the National Classification Scheme,[23] a

---

19 Office of the eSafety Commissioner (2018), State of Play – Youth, Kids and Digital Dangers, available at: https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf.

20 Office of the eSafety Commissioner (2019), Safety by Design Overview, available at: https://www.esafety.gov.au/sites/default/files/2019-10//SBD%20-%20Overview%20May19.pdf?v=1718071814913.

21 Office of the eSafety Commissioner (2019), Safety by Design Overview, 4.

22 Office of the eSafety Commissioner (2024), What is illegal and restricted online content?. Available at: https://www.esafety.gov.au/report/what-is-illegal-restricted-content#:~:text='Illegal%20and%20restricted%20online%20content,activity%2C%20detailed%20nudity%20or%20high

23 The National Classification Scheme is an agreement between the Australian, state and territory governments. The Federal Minister for Communications, and the state and territory Ministers responsible for classification oversee the Scheme. The Scheme defines the roles of the Commonwealth, states and territories in deciding ratings and enforcement.

cooperative arrangement between the Australian Government and State and Territory governments for the classification of films, computer games, and certain publications.

Material which promotes, incites, instructs in or depicts abhorrent violent conduct

Under the *Criminal Code Act 1995*, the eSafety Commissioner can assess whether online content is 'Abhorrent Violent Material'. In such a case, the Commissioner can issue a notice to any website or hosting service that provides access to the content, directing them to remove it. Where a service is later prosecuted for failing to remove or cease hosting material, the notice can be used in legal proceedings to show recklessness regarding the content.[24] The eSafety Commissioner recently exercised these powers in relation to content depicting the stabbing of a religious leader at Wakeley in Sydney on 15 April 2024.

Non-consensual sharing of intimate images and image-based abuse

The role of social media platforms and online forums as a gateway to the online grooming, sexual solicitation, and uploading of sexually explicit photos or videos of children is widely recognised.

Image-based abuse refers to a person sharing, or threatening to share, an intimate image or video of a person without their consent.[25] The image or video can be real, or altered or faked to look like the targeted person, or shared in a way that makes others think it is the targeted person, even when it is not (such as a nude of someone else tagged with their name).

Section 15 of the *Online Safety Act* defines 'intimate image'. It is unnecessary to reproduce that definition here.

---

24 Office of the eSafety Commissioner (2024), What is illegal and restricted online content?.

25 Office of the eSafety Commissioner, *FAQ about image-based abuse*, published 2024, available at: https://www.esafety.gov.au/key-topics/image-based-abuse/faq-about-image-based-abuse (accessed on 12 June 2024).

The impact of social media on children's development

There is evidence that there are two critical periods for neural development in children and young people: the first occurs in the first year of a child's life, and the second starts at the outset of puberty until early adulthood (10 to 25 years old).[26]

During the second period, children crave social rewards, such as visibility, attention, and positive feedback from peers, which coincides with the time they start to interact with social media and other online platforms. During this period, areas of the brain responsible for inhibiting behaviour are not fully developed until early adulthood.

Some researchers have likened children and young people's interaction with social media with 'empty calories', where biological and psychological needs are satisfied without the addition of health benefits.[27]

This has implications for children and young people's interactions with social media stimuli (such as receiving 'likes' or followers, which activates the social reward regions of the brain), which effectively, 'capitalize on youths' biologically based need for social rewards before they are able to regulate themselves from over-use.[28]

Evidence provided in 2023 to the US Senate Committee on Protecting Our Children Online suggests there are at least four significant consequences for youth mental health: increased feelings of loneliness, heightened risk for negative peer influence (in relation to engaging with illegal, violent, or abhorrent online content), risks for addictive social media use, and alterations in brain development[29].

There appear to be differences across age groups in relation to the effects that social media use has on life satisfaction. In a UK study, published in 2022 of over 17,000 young people, aged ten to 21 years, it was found that the detrimental effects of high levels of social media use may

---

26 K Mils, (2023), *APA chief scientist outlines potential harms, benefits of social media for kids*, American Psychological Association, 6. Available at: https://www.apa.org/news/press/releases/2023/02/harms-benefits-social-media-kids,

27 Prinstein, M (2023), *Written testimony of Mitch Prinstein, PhD, ABPP, Chief Science Officer, American Psychological Association, Protecting our Children Online, Before the US Senate Committee on Judiciary. Available at: https://www.apaservices.org/advocacy/news/testimony-prinstein-protecting-children-online.pdf?utm_source=apa.org&utm_medium=referral&utm_content=/news/press/releases/2023/02/harms-benefits-social-media-kids.*

28 Mils, K (2023), 7.

29 Mils, K (2023), 7–10

be especially pronounced at ages 14–15 years, and 19 years for boys, and 11–13 years and 19 years for girls.[30]

Perspectives from clinical psychology

Dr Danielle Einstein, a clinical psychologist and Adjunct Fellow at the School of Psychological Science at Macquarie University met with the Examiner. In a useful summary she contended that, in relation to 13 to 15 year olds, the intensity of social media amplified social hierarchy favouring socially mature teens and disadvantaging others in school communities. The harms created in vulnerable teens were not helpful for social skills and anxiety or resilience. She questioned the utility of individual pieces of academic research and literature reviews. Theory had to be combined with research and examination of widespread experiences in order to guide sensible public policy.

Dr Einstein spoke of what she called the 'bidirectional relationship' between screen time and mental health, a phenomenon referred to in a submission by Blackdog/ReachOut and Headspace to the Joint Select Committee on Social Media and Australian Society. It was evident that limiting screen use benefited adolescents with mental health difficulties, helping them engage in other activities and build resilience. Evidence-based treatments of anxiety and depression prioritised scheduling of activities in the real world to pass time (for depression) and to face and overcome fears (for anxiety).

She contested the suggestion that social media is a safe haven for social connection, a suggestion which, she argued, ignores the risk of over-dependence on social media. That can prevent skill building and will prevent real life social engagement.

Further, fear of missing out was said to be strongly linked with compulsive social media use, negatively impacting on social wellbeing and increasing anxiety.

Under the heading 'Proposals for Change' Dr Einstein suggested that raising the age of social media use to 16 would protect vulnerable teens, support parents and school communities and promote healthier development.

---

30 Ofcom, *Children and parents: media use and attitudes report*, 2022. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf

Associate Professor Melanie Turner, who is Deputy Chief Psychiatrist, for South Australia, said that overall the largest issue with social media was that it allowed children and adolescents access to a volume of information that they were not developmentally ready to understand or interpret. Before exposure to a large amount of data on social media, children's exposure to sights, sounds and experiences were those offered by their families, friends and schools. If no one in their circle talked about self-harming, they were not exposed to it. Online there could be exposure to self-harming. A child so exposed would experience something in isolation away from context and support and an adult framework to interpret it. There would not be a safety net or filter by way of a parent or carer to intercept, realign or reshape the experience. The spaces that were most unsafe from the point of view of the Deputy Chief Psychiatrist were large user programs where the child would be able to view content by anyone with no filters. Even if a child did not make content, they were exposed as a vulnerable user. Associate Professor Turner identified sites which she contended were unsafe and should not be accessible ideally to those under 16, but under 14 if that were the limit. She listed TikTok, YouTube, Instagram, Snap Chat, Facebook, WhatsApp and Kik. She also suggested that Discord can be a problem for open chat settings although most gamers use the VOIP to talk during gaming and to also instantly message.

Aboriginal and Torres Strait Islander Children online

April Lawrie is the inaugural Commissioner for Aboriginal Children and Young People of South Australia. She leads work promoting the rights, development and wellbeing of Aboriginal children and young people within South Australia. Her role is established under the *Children and Young People (Oversight and Advocacy Bodies) Act 2016*. She is guided by the United Nations Convention on the Rights of the Child, and promotes and advocates for the rights, interests and wellbeing of Aboriginal children and young people in South Australia in the realm of their indigeneity with a view to ensuring that as part of the global community, South Australia enacts its obligations to these two Covenants.

Reference was made to research commissioned by eSafety in 2021 to explore the opportunities and risks that the Internet presents for children in Australia. Key findings included that:

- Aboriginal and Torres Strait Islander children are highly engaged in the digital environment. They use the Internet to connect with friends and relatives, expand social

networks, share creative content and discuss global issues. The Internet also serves as a vital source of health information and emotional support.

- Despite positive experiences there are risks:

  Aboriginal and Torres Strait Islander children face exposure to harmful content, including hate speech;

  Such exposure can impact mental health, school work and overall wellbeing.

- Many parents and caregivers of Aboriginal and Torres Strait Islander children actively engage in 'digital parenting'. They are more likely to be aware of their child being exposed to negative material and hate speech online than parents and caregivers of Australian children overall. The research was said to show that parents and caregivers of Aboriginal and Torres Strait Isander children actively foster their child's Internet activity doing online activities together and encouraging them to learn and explore online. They are aware of negative material and hate speech online. They encourage safe Internet use and explore online activities together.

Commissioner Lawrie presented a Youth Voices Report in 2021 to South Australia's Minister for Education. It set out issues impacting the lives of Aboriginal children and young people as expressed by them.

Social media was listed as number 10 of a list of top ten topics selected by Aboriginal children indicating issues that worry them. There were references to the perceived benefits and disadvantages of social media. The Commissioner's comment was:

> The Aboriginal children and young people I spoke with can be described as part of the 'social media generation'. They have grown up in a time where technology improves at a rapid pace and requires constant adaptability. They frequently use social media platforms such as Snapchat, TikTok and Instagram to connect with and maintain relationships with family and friends. Some Aboriginal young people told me about the negative effects social media can have on their mental health and self-image.[31]

Balancing risks and benefits — the eSafety Commissioner

[31] South Australia's Commissioner for Aboriginal Children and Young People Report 2021: Youth Voices Report', 31 October 2022, 45

In her submission in June 2024 to the Joint Select Committee on Social Media and Australian Society, the eSafety Commissioner observed that a discussion about the risks of social media should be balanced with a discussion of the benefits. To quote from her submission:

> Social media may also provide a range of opportunities that are protective of mental health, such as inclusion, social connection and belonging. These benefits are especially important for young people who experience difficulties with participation and social inclusion in other contexts.
>
> For example eSafety's research into the online experiences of Aboriginal and Torres Strait Islander children, the digital lives of young people with disability, and our report on LGBTQI+ teens, highlights some of the ways online environments can help facilitate connection, support and cultural expression.[32]

The point was made that the relationship between mental health and social media is complex and the evidence base for the relationship is still evolving. The impact of social media is not the same for everyone. Young users vary considerably in their uses of social media. This was said to include the platforms they access, the digital features they are exposed to, the content they consume and the communities they engage with.

The impact of their online experiences is also highly individualised. Restrictive measures that may benefit one child may be ineffective or even harmful for another. The eSafety Commissioner submitted:

> This makes decisions about preventing or limiting children's access or participation online incredibly complex. These decisions require thorough consideration of solutions that do not inadvertently introduce negative outcomes.
>
> Additionally, most of the evidence and recommendations available are based on international research. There is a need to review and weigh the Australian evidence base and consider the extent to which international evidence and advisories are generalisable to the Australian context.[33]

To ban or not to ban

In 2022, the Office of the eSafety Commissioner cautioned against prohibiting access by children and young people to social media altogether:

> An abstinence-based approach of cutting off young people from the internet is likely to have adverse consequences for the mental health and wellbeing of children and young people not from supportive homes with engaged parents. Moreover, it could shut vulnerable young people off from support services and affinity groups that could

[32] eSafety Commissioner, 'eSafety submission to the Joint Select Committee on Social Media and Australian Society, 21 June 2024, 10.

[33] eSafety Commissioner, eSafety submission to the Joint Select Committee on Social Media and Australian Society, 21 June 2024, 10.

> help them achieve a sense of understanding and belonging. Such blunt force approaches could also prevent young people who are excluded from developing the key skills they will need to navigate the online world safely as adults".[34]

The eSafety Commissioner is not alone in that view. Similar views have been expressed by a number of other public officers and academics. There are also strong views to the contrary.

Comment

It is not within the remit of this Examination to canvass the merits of the South Australian Government's policy position. It is uncontroversial that there are risks and benefits in young people's exposure to social media services. Accordingly, there are costs and benefits associated with a legislated restriction. Judgment about where the balance lies is a matter for the South Australian Government. Nevertheless it is an object of this Examination to consider a legislative mechanisms by which the disadvantages of restriction can be mitigated. The principal technique for mitigation is to provide a mechanism whereby safe and beneficial social media services can be exempted from the restriction and the development of such services can be encouraged.

[34] eSafety Commissioner, Inquiry into Social Media and Online Safety, January 2022, 27.

Chapter 3: The meaning of the term 'social media', its evolution and variety

Introduction

In considering a legislative model for an age-based restriction on access to 'social media' it is necessary to consider the scope of that term. That is done by reference to its history, its general usage and examples of how it is defined in legislation. This chapter of the Report considers its history and general usage. It is not a treatise on the subject, but indicative of the range of the term 'social media'.

A very brief history

Social media can be regarded as an evolution of communications mechanisms dating back over 2,000 years.[35] It has been suggested that the invention of morse code in the 1840s was a step in that evolution.[36] Twentieth century social media precursors included CompuServe — a business created mainframe computer communication solution, which entered the public domain in the late 1980s; APARNET, a digital network created by the US Department of Defence[37] and 'NSFNET', a network established by the National Science Foundation in the United States in 1987. It has been suggested that the term 'social media' may have first been applied to a Tokyo online media environment called Matisse in 1994.[38]

Early social networks based on web technology were Classmates.com and SixDegrees.com.[39] Classmates.com was founded in 1995 and created social networks between members of high school and college graduating classes, Armed Service branches and workplaces. SixDegrees.com, launched in 1997, was said to be 'the first true social networking site'. Members could create their own profiles and lists of friends and use a private message system to get in touch with each other. SixDegrees.com collapsed with many other .coms in 2000.

---

35 Tom Standage, *Writing on the Wall: Social Media – The First 2,000 Year*s (Bloomsbury, USA, 2013).

36 Michael S Rosenwald, 'Before Twitter and Facebook there was Morse Code: Remembering Social Media's True Inventor', *Washington Post* (24 May 2017) https://www.washingtonpost.com/news/retropolis/wp/2017/05/24/before-there-was-twitter-there-was-morse-code-remembering-social-medias-true-inventor/.

37 *The Evolution of Social Media: How did it begin and where could it go next?*', (Blog Post, 28 May 2020). Maryville University Online https://online.maryville.edu/blog/evolution-social -media/

38 T Aichner, M Grunfelder, .M Maurer and D Jegeni, 'Twenty Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019', Cyber Psychology Behavioural Social Network, 24(4) April 2021, 215–22.

39 Encyclopedia Britannica Online, https://www.britannica.com. Accessed 9 August 2024.

Social network sites such as Friendster and Myspace, which became popular in the early 2000s, provided connections for family members, friends and acquaintances. They were overtaken by Facebook. Other forms of social media emerged which provided for the sharing of specific types of content — YouTube for videos, TikTok for short videos and LinkedIn for resumes and professional connections. The social media landscape in the 21st century continues to evolve.

In delivering the opinion of the Supreme Court of the United States in *Moody v NetChoice LLC*,[40] published on 1 July 2024, Justice Kagan noted that 30 years ago the Court felt the need to explain to the opinion-reading public that the 'Internet is an international network of interconnected computers'. Things had changed since then. At that time only 40 million people used the Internet. Today, she pointed out, Facebook and YouTube alone have over 2 billion users each. The Judge observed

> These years have brought a dizzying transformation in how people communicate, and with it a raft of public policy issues. Social media platforms, as well as other websites, have gone from unheard-of to inescapable. They structure how we relate to family and friends, as well as to businesses, civic organizations, and governments. The novel services they offer make our lives better, and make them worse—create unparalleled opportunities and unprecedented dangers. The questions of whether, when, and how to regulate online entities, and in particular social-media giants, are understandably on the front-burner of many legislatures and agencies. And those government actors will generally be better positioned than courts to respond to the emerging challenges social-media entities pose.[41]

The challenge of definition

In a critical history of social media entitled 'The Culture of Connectivity: A Critical History of Social Media' published by Oxford University Press in 2013, José van Dijck, Professor of Media and Digital Society at Utrecht University and a leading international expert in the field, wrote of the extraordinary growth in the number of users worldwide of social media sites in the second decade of the 21st century.

Relevant to the repeated claims of the importance of connectiveness which have informed the views of sceptics of a ban on children's access, she observed that it was the need for connectiveness that drove many users to the sites. When Web 2.0 first marshalled the development of social media:

---

40 *Moody v NetChoice, LLC.*, 603 US (2024).

41 603 US (2024) 2

> Participatory culture was the buzzword that connoted the Web's potential to nurture connections, build communities, and advance democracy. Many platforms embraced this rekindled spirit when they started to make the Web 'more social'.[42]

Professor van Dijck pointed to the evolutionary development involving the incorporation of sites by existing and new information companies, often less interested in communities of users than in their data — a by-product of making connections and staying connected online:

> *Connectivity* quickly evolved into a valuable resource as engineers found ways to code information into algorithms that helped brand a particular form of online sociality and make it profitable in online markets — serving a global market of social networking and user-generated content. Large and influential platforms such as Facebook, Twitter, YouTube, and LinkedIn exploded in terms of users and monetizing potential, alongside countless smaller profit and nonprofit sites.[43]

She described the emergence of an ecosystem of connective media with a few large and many small players.[44] It was a common fallacy to think of platforms as merely facilitating networking activities. The construction of platforms and social practices were 'mutually constitutive'. Many habits now permeated by social media platforms used to be ordinary, informal manifestations of social life. Examples were:

> Talking to friends, exchanging gossip, showing holiday pictures, scribbling notes, checking on a friend's well-being, or watching a neighbor's home video.[45]

These were acts commonly shared with selected individuals:

> A major change is that through social media, these casual speech acts have turned into formalized inscriptions, which, once embedded in the larger economy of wider publics, take on a different value. Utterances previously expressed offhandedly are now released into a public domain where they can have far-reaching and long-lasting effects. Social media platforms have unquestionably altered the nature of private and public communication.[46]

In a more recent work, van Dijck and others discussed the larger concept of the online platform — 'a programmable digital architecture designed to organize interactions between users — not just end-users but also corporate entities and public bodies.'[47] Examples not necessarily

---

42 José van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press, 2013) 4.

43 Ibid.

44 Ibid.

45 Van Dijck, above n 42, 7.

46 Van Dijck, above n 42, 7.

47 Jose Van Dijck, Thomas Poell, Martijn de Waal, *The Platform Society: Public Values in a Connected World* (Oxford University Press, 2018) 4.

included within the general understanding of 'social media' include AirbnB, Uber and Deliveroo.

The platform is 'geared towards the systematic collection, algorithmic processing, circulation and monetization of user data.'[48] There is a platform ecosystem said to be operated in the West by a small number of big tech companies — Alphabet, Google, Apple, Facebook, Amazon, and Microsoft. Their infrastructure services are said to be central to the overall design of the ecosystem, albeit they are not the only players.

The challenge of definition

The rapid evolution of social media generates a difficult question of definition for policy makers and legislators. Thomas Aichner, who published a review of relevant literature on social media in 2020, made the important observation that:

> SM cover a broad variety of scopes with specific functions and applications that can differ greatly between the different types of SM. Consequently, also the purpose and users' perceived value of using SM varies.[49]

An evident commonality of all types of social media is socialisation between the users. Interacting users may be family members and friends. At the time of Aichner's study close to 100% of larger corporations were using a social media platform to inform customers, gather information, receive feedback, provide after sales services or consultancy and promote products or services. The key characteristic was two-way communication between brand and customer. Another application connects jobseekers with employers. Most Fortune 500 companies use LinkedIn for talent acquisition.[50]

This background led to the research question explored by Aichner namely whether those who studied SM had the same definition in mind when talking about social media and social network online communities? The study considered how the content of the term had changed from 1994 to 2019. A helpful table set out major definitions of social media and analogous terms formulated in academic literature published in that period.

---

48 Ibid.
49 Aichner, above n 38 (footnote omitted).
50 Ibid (footnote omitted).

Year	Definition	Author	Source	Google scholar citation
1996	When computer networks link people as well as machines, they become social networks, which we call **computer-supported social networks** (CSSNs).	Wellman	Annual Review of Sociology	1,886
1997	**Virtual communities** are groups of people who communicate with each other via electronic media and are a relatively new phenomenon.	Room et al.	International Journal of Information Management	384
1997	When a computer network connects people or organizations, it is a **social network**. Just as a computer network is a set of machines connected by a set of cables, a social network is a set of people (or organizations or other social entities) connected by a set of social relationships, such as friendship, co-working, or information exchange.	Garton et al	Journal of Computer Mediated Communications	2,158
1999	**Virtual communities** are defined by bringing people together with a common set of needs or interests. Those needs or interests could span a variety of dimensions. Virtual communities could be organized around an area of interest (such as sports or stock investments), a demographic segment (certain age groups within the population), or a geographic region (metropolitan areas).	Hagel	Journal of Interactive Marketing	3,325
2001	For the purposes of this article, we define a **virtual community** (in a relatively neutral way) as any entity that exhibits all of the following characteristics: (a) It is constituted by an aggregation of people. (b) Its constituents are rational utility-maximizers. (c) Its constituents interact with one other without physical collocation, but not every constituent necessarily interacts with every other constituent. (d) Its constituents are engaged in a (broadly defined) social-exchange	Balasubramanian and Majahan	International Journal of Electronic Commerce	699

	process that includes mutual production and consumption (e.g., mutual dissemination and perusal of thoughts and opinions). Although each of its constituents is engaged in some level of consumption, not all of them are necessarily engaged in production. Such social exchange (as opposed to monetary or material exchange) is a necessary, but not always the only, component of interaction between the constituents of the entity. (e) The social interaction between constituents revolves around a well-understood focus that comprises a shared objective (e.g., environmental protection), a shared property/identity (e.g., a national culture or a lifestyle choice), or a shared interest (e.g., a hobby).			
2002	**Virtual communities** can be defined as groups of people with common interests and practices that communicate regularly and for some duration in an organized way over the Internet through a common location or mechanism. The location of the virtual community, although not physical, is important because it establishes the virtual "place" where the members meet. This location or mechanism may be a chatroom, bulletin board, or listserv e-mail program.	Ridings et al	The Journal of Strategic Information Systems	1, 891
2005	SNSs [**social networking services**] are designed specifically to facilitate user interaction for a variety of goals, mainly dating, business networking, and promotion	Marwick	Conference Association of Internet Res. 6.0	146
2006	At the most basic level, an **online social network** is an Internet community where individuals interact, often through profiles that (re)present their public persona (and their networks of connections) to others.	Acquisiti and Gross	Conference Privacy Enhancing Technologies (PET)	2, 680

2007	A **social networking site** (SNS) connects and presents people based on information gathered about them, as stored in their user profiles.	O'Murch u et al	Book Viral Marketing Concepts and Cases	263
2007	**Social network sites** are web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and traverse their list of connections and those made by others within the system.	Boyd and Ellison	Journal of Computer-Mediated Communication	19,908
2008	**Social networking sites** typically provide users with a profile space, facilities for uploading content (e.g., photos, music), messaging in various forms, and the ability to make connections to other people.	Joinson	Conference Proceedings of the SIGCHI Conference on Human Factors in Computing Systems	2,284
2009	**Social network sites** provide a public forum that enables the exchange of digital information, such as pictures, videos, text, blogs, and hyperlinks between users with common interests, such as hobbies, work, school, family, and friendship.	Sledgian owski and Kulviwat	Journal of Computer Information Systems	668
2010	**Social media** is a group of Internet-based applications that builds on the ideological and technological foundations of Web 2.0, and that allows the creation and exchange of user-generated content.	Kaplan and Haenlein	Business Horizons	19,656
2011	**Social media** is a honeycomb of seven functional building blocks: identity, conversations, sharing, presence, relationships, reputation, and groups.	Kietzman n et al	Business Horizons	5,174
2012	**Social networking sites** can be defined as virtual collections of user profiles that can be shared with others	Hughes et al	Computers in Human Behavior	1,079
2013	A **social network site** is a networked communication platform in which participants (a) have uniquely identifiable profiles that consist of user-supplied content, content	Ellison and Boyd	Book: The Oxford Handbook of Internet Studies	1,118

	provided by other users, and/or system-level data; (b) can publicly articulate connections that can be viewed and traversed by others; and (c) can consume, produce, and/or interact with streams of user-generated content provided by their connections on the site.			
2015	**Social media** are Internet-based, disentrained, and persistent channels of masspersonal communication facilitating perceptions of interactions among users, deriving value primarily from user-generated content.	Carr and Hayes	Atlantic Journal of Communications	386
2016	**Social media** is the colonization of the space between traditional broadcast and private dyadic communication, providing people with a scale of group size and degrees of privacy that we have termed "scalable sociality."	Miller et al	Book: How the World Changed Social media	568
2018	For this study, we define "**social-media**" as Web sites and technological applications that allow its users to share content and/or to participate in social networking.	Leyrer-Jackson and Wilson	Journal of Biological Education	17
2018	**Social media** is made up of various user-driven platforms that facilitate diffusion of compelling content, dialogue creation, and communication to a broader audience. It is essentially a digital space created by the people and for the people, and it provides an environment that is conducive for interactions and networking to occur at different levels (for instance, personal, professional, business, marketing, political, and societal).	Kapoor et al	Information Systems Frontiers	293
2019	For purposes of this chapter, we define **social media** as any online resource that is designed to facilitate engagement between individuals.	Bishop	Book: Consumer Informatics and Digital Health	4

A constant feature of the definitions has been the role of social media in enabling human interaction. The emphasis has changed from 'people' to 'users' and to the generation and sharing of content. Before 2009 the common interests that linked people were a feature of social media. That link is said to have gone missing after 2010. Aichner and his colleagues observed that a result of the evolving landscape of social media was that few scholars had made an effort to develop a definition.

Although not within the ordinary understanding of social media discussed thus far, online gambling platforms present risks for children and adolescents. In a paper published in the *British Medical Bulletin* in 2020, reference was made to a report of the UK Gambling Commission 2019 which indicated that online gambling had increased in frequency in that year with 7% reporting gambling online and 5% of 11-16 year olds stating that they had played national lottery games online and/or other gambling websites using their parents' account with their permission.

An interesting observation was made about the link between online video games and the early onset of gambling. The latest edition of the *Diagnostic and Statistical Manual of Mental Disorders*[51] tentatively recognised the existence of 'internet gaming disorder'. There are, however, difficulties with the definition. The researchers who published in the *British Medical Bulletin* observed that:

> Adolescents are receptive to modern forms of gambling because of the apparent similarity between these games and other familiar technology-based games.[52]

The preceding taxonomical review and the Aichner paper highlight the importance, in any legal regulation of 'social media', of identifying the genus relevant to the policy. Consistently with the Terms of Reference, that policy is the protection of children from the harmful effects on their wellbeing and mental health flowing from the use of social media. The definition should allow for regulatory coverage responsive to the evolution of social media and the generation of new species within the genus. It is not suggested that the definition should extend to all species of online platform as that may involve an unduly extensive and complex regulatory coverage. Consistently with the government policy, the coverage of any legislative restriction should not

---

51 (2013, 5th ed).

52 Allan M Edmond and Mark D Griffiths, 'Gambling in Children and Adolescents' (2020) 136 *British Medical Bulletin* 21–29.

extend to social media services or platforms which do not expose children in the relevant age ranges to harms of the kind identified in the Terms of Reference.

Some examples of recent named species within the genus of social media, as generally understood, follow.

The varieties of social media in use today — the species

A list published to business audiences set out the following in a blog published in November 2023.[53]

1. Social networking sites

Examples: Facebook, LinkedIn, X (formerly Twitter), Threads

Used for: Sharing both text and visual content to disseminate information and facilitate networking, event promotion, and advertising.

2. Image-based social media

Examples: Instagram, Pinterest, Snapchat, TikTok

Used for: Visual story-telling, brand building, and social commerce (users can shop in-app, rather than being directed to a website to make an online purchase, e.g., Instagram Shopping, Pinterest Shopping, Snapchat Store). Users can generally add music to soundtrack their images, and viewers can either swipe through each photo or let them scroll automatically.

3. Short-form video social media

Examples: Instagram Reels, TikTok, YouTube Shorts

Used for: Sharing short-form video content (usually between five seconds and ninety seconds long.

4. Livestream social media

Examples: Facebook Live, Instagram Live, TikTok Live, Twitch, YouTube

[53] Sarah Israel, '7 Types of Social Media and How Each Can Benefit Your Business', 8 November 2023. https://blog.hootsuite.com/types-of-social-media/. Accessed 9 August 2024.

Used for: Broadcasting live video to many viewers at one time (e.g., to launch new products, interview guests, or host Q&A sessions with audience).

5. *Discussion forums*

Examples: Reddit, Quora

Used for: Asking and answering questions, networking, building communities around needs and interests.

6. *Private community platforms*

Examples: Discord, Facebook Groups, Patreon, Slack

Used for: Establishing a community of members that is not open to the public.

7. *Decentralised social networks*

Examples: Bluesky, Mastodon

Used for: Building communities outside traditional social networking sites like Facebook and X. For example, Mastodon is a decentralised social network that consists of independent services organised around specific themes, topics or interests. In contrast, social media platforms like Facebook and X are centralised, meaning they are typically owned and operated by a single company.

It is not suggested that the above list is exhaustive, authoritative, or definitive. It is, however, indicative of a perception of the principal classes of social media and examples of social media services within those classes.

Professor van Dijck in her work selected a non-exhaustive list of four different types of social media relevant to her analysis. These were:

1. *Social network sites (SNS*)

Those sites primarily promote inter-personal contact between individuals or groups, forging personal, professional or geographical connections and encouraging weak ties. Examples given were Facebook, Twitter, LinkedIn, Google+ and Foursquare.

2. *Sites for user-generated content (UGC)*

Those sites support creativity, foreground cultural activity and promote the exchange of amateur or professional content. They include YouTube, Flickr, Myspace, GarageBand, and Wikipedia.

3. *Trading and marketing sites (TMSs)*

Principally aimed at exchanging products or selling them. Noteworthy examples were Amazon, eBay, Groupon and Craigslist.

4. *Play and game sites (PGS)*

This category is a flourishing genre with popular games including FarmVille, CityVille, The Sims Social, Word Feud and Angry Birds.

Professor van Dijck observed that there are no sharp boundaries between the categories. The carving out and appropriation of one or more specific niches is said to be 'part of the continuous battle to dominate a segment of online sociality.'[54] Facebook, whose prime target was to promote social networking also encouraged its users to add creative products. Examples given were photos and short videos. YouTube, which was set up to generate creative content by users, could also be viewed as an SNS because of the sharing of specific postings between communities such as anime videos. Although Google had tried to turn YouTube into an SNS, it remained primarily a site for UGC. The search company thus started its own social networking services Google+ in May 2011. Facebook and Google both seek to expand their platforms with commercial and game services through partnerships and takeovers so they become players in the TMS and PGS branches.[55]

Comment

This dynamic landscape suggests that any regulatory regime should be capable of adaptation to change — where, for example, a safe social media service exempted from its coverage evolves into a social media service which exposes child users to risk.

[54] Van Dijck, above n 42, 8.
[55] Van Dijck, above n 42, 9 .

Dictionary definitions of 'social media'

Dictionary definitions of social media can be indicative of the current 'ordinary meaning' of the term. A non-exhaustive review of dictionary definitions follows.

Merriam-Webster Online

> Forms of electronic communication (as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).

Cambridge Dictionary (Online)

> Websites and computer programs that allow people to communicate and share information, opinions, pictures, videos etc on the internet especially social networking websites.

The *Oxford English Dictionary (Online)*

> Websites and applications which enable users to create and share content or to participate in social networking.

Oxford Reference: A Dictionary of Media and Communication

This dictionary published online in 2011 defines 'social media' thus:

> A broad category or genre of communications media which occasion or enable social interaction among groups of people, whether they are known to each other or strangers, localized in the same place or geographically dispersed. It includes new media such as newsgroups, MMOGs, and social networking sites. Such media can be thought of metaphorically as virtual meeting places which function to occasion the exchange of media content among users who are both producers and consumers. Social media have also become adopted as a significant marketing tool.

Oxford Reference: A Dictionary of Social Media (2016 Online publication)

The Oxford Reference Dictionary: A Dictionary of Social Media defines 'social media tools' as:

> The online and mobile technologies or platforms people use to interact and share content, including social networking sites, social bookmarking and social news sites, geo social networking sites, blogs, online forums, file sharing and media-sharing sites, social gaming sites, social commerce sites, virtual worlds and Wikis.

There is a related term 'social media platforms' which is defined as:

> The online or mobile systems available for some particular purpose (such as advertising or publishing): either the general types (blogs, social networking sites, online forums etc), or particular apps.

There is a distinction drawn between computer-based social media and mobile social media. Computer-based social media is defined as 'social apps accessed through the internet using computers as distinguished from mobile social media.' Mobile social media is:

> Apps or services accessed through mobile devices, enabling users to share information, news and other content. Such media are often distinguished from computer-based (or online) social media such as in relation to design issues, but cross-platform social media include Twitter and Facebook.

Legal definitions of social media

The 6th edition of the *LexisNexis Concise Australian Legal Dictionary*, published in 2021 defines 'social media' as:

> An internet-based or mobile broadcasting-based technology or application through which users can create and share content.
>
> …
>
> Social media technologies are web-based services or mobile phone applications that facilitate social interaction. They allow users to find and interact with other users with common interests and share opinions, experience and user generated content, such as videos, photographs, and text messages.

The term 'social networking platform' is also defined:

> A social media service that is designed to allow users to create an online relationship network in order to exchange information and engage with others who share a common interest.

Examples of 'social networking platforms' are Facebook, LinkedIn, WhatsApp, Twitter, Instagram and Snapchat. Social networking platforms are one of three types of platforms on the media and advertising services market, the other two being digital search engines (software systems design to search for information on the World Wide Web, for example, Google Search and Yahoo) and other digital content aggregation platforms such as Google News and Apple News which collect information from disparate sources and present them as a collated, curated product.

Black's Law Dictionary defines 'social media' as:

> Any cell phone or internet based tools and applications that are used to share and distribute information. Sites such as Facebook, Twitter, YouTube, blogs.[56]

There are no citations to that definition.

In the opinion she delivered for the Supreme Court of the United States on 1 July 2024 in *Moody v NetChoice*, Justice Kagan said:

> As commonly understood, the term "social media platforms" typically refers to websites and mobile apps that allow users to upload content—messages, pictures, videos, and so on—to share with others. Those viewing the content can then react to it, comment on it, or share it themselves. The biggest social-media companies—entities like Facebook and YouTube—host a staggering amount of content.[57]

The Florida law in issue in that case provided an expansive definition of 'social media platforms' covering 'any information service, system, Internet search engine or access software provider' that '[p]rovides or enables computer access by multiple users to a computer server, including an Internet platform or a social media site.'[58] The Texas law also in issue there, regulated any social media platform having over 50 million monthly active users that allowed its users 'to communicate with other users for the primary purpose of posting information, comments, messages or images'.[59] It should be noted that the case concerned challenges to laws which sought to restrict moderation by providers of online content. The First Amendment of the American Constitution was in play.

Against that background, it is necessary to review the leading statutory definition used in Australia's *Online Safety Act* and statutory definitions appearing in other national and sub-national jurisdictions.

---

56 Black's Law Dictionary Free, 2nd ed.
57 *Moody v NetChoice, LLC*, 603 US (2024) 5.
58 Florida Statute No 501.2041 (1)(g)(1).
59 Tex. Bus and Com Code Ann § 120.001(1), 120.002 (b).

Chapter 4: The leading Australian statutory definition of 'social media service' and related terms

Introduction

The *Online Safety Act* is the principal Commonwealth law regulating social media. The legislative scheme of that Act is discussed later in this Report. It is important that statutory terms defining regulatory coverage in South Australian legislation should be, so far as possible, compatible with those used in the national legislation. That is particularly so if any South Australian legislation is to act as a stimulus for the development of a national scheme in relation to access to social media by children. The Commonwealth Act adopts a definition which, on its face, appears to be sufficiently generic to be applicable in any proposed South Australian legislation. It also appears to be sufficiently general to give effect to the South Australian policy setting, albeit it will be necessary to calibrate its scope by creating a mechanism under which child safe social media services can be exempted from its coverage.

Definition of 'social media' in the Online Safety Act

The *Online Safety Act* defines the term 'social media service' in s 13 as follows:

> (1) For the purposes of this Act, ***social media service*** means:
>
> (a) an electronic service that satisfies the following conditions:
>
> (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users;
>
> (ii) the service allows end-users to link to, or interact with, some or all of the other end-users;
>
> (iii) the service allows end-users to post material on the service;
>
> (iv) such other conditions (if any) as are set out in the legislative rules; or
>
> (b) an electronic service specified in the legislative rules;
>
> but does not include an exempt service (as defined by subsection (4)).
>
> Note: Online social interaction does not include (for example) online business interaction.
>
> (2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes.
>
> Note: Social purposes does not include (for example) business purposes.

(3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes:

(a) the provision of advertising material on the service;

(b) the generation of revenue from the provision of advertising material on the service.

Exempt services

(4) For the purposes of this section, a service is an ***exempt service*** if:

(a) none of the material on the service is accessible to, or delivered to, one or more end-users in Australia; or

(b) the service is specified in the legislative rules.

The concept of an 'exempt service' can be applied in an expanded form to define the application of the South Australian law so that it does not prevent access to entirely beneficial or largely risk-free services, determined by category or individual designation effected by way of ministerial notice.

'Social media service' as defined in s 13(1) is a species of 'electronic service'. That term is defined in s 5 of the Act:

Electronic service means:

(a) a service that allows end-users to access material using a carriage service; or

(b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service;

but does not include:

(c) a broadcasting service; or

(d) a datacasting service (within the meaning of the *Broadcasting Services Act 1992*).

This definition excludes 'broadcasting services' and 'datacasting services' from the definition of electronic service and therefore from the definition of social media service. Definitions in s 5 of the *Online Safety Act* of 'broadcasting services' and 'datacasting services' generally cover standard television or radio programming.

Another key concept in the *Online Safety Act* is that of a 'relevant electronic service', which is defined in s 13A as:

Relevant electronic service

(1) For the purposes of this Act, ***relevant electronic service*** means any of the following electronic services:

(a) a service that enables end-users to communicate, by means of email, with other end-users;

(b) an instant messaging service that enables end-users to communicate with other end-users;

(c) an SMS service that enables end-users to communicate with other end-users;

(d) an MMS service that enables end-users to communicate with other end-users;

(e) a chat service that enables end-users to communicate with other end-users;

(f) a service that enables end - users to play online games with other end-users;

(g) an electronic service specified in the legislative rules;

but does not include an exempt service (as defined by subsection (2)).

Note 1: ***SMS*** is short for short message service.

Note 2: ***MMS*** is short for multimedia message service.

Exempt services

(2) For the purposes of this section, a service is an ***exempt service*** if none of the material on the service is accessible to, or delivered to, one or more end-users in Australia.

The definition of 'relevant electronic service' is pertinent as not all such services will automatically be 'social media services'. The powers in the *Online Safety Act* typically apply in relation to social media services and relevant electronic services, covering a wide range of digital interaction methods. If a South Australian law on social media used an equivalent definition to the *Online Safety Act*, (i.e. not necessarily covering the categories within the definition of relevant electronic service) it would not cover services such as chat apps or social features in online video games. Policy questions would arise as to the intended scope of the reform as regards these services (for example, could a minor under the prescribed age use the Facebook messenger app without parental permission but not the main Facebook app?).

Two other definitions of relevance which appear in s 5 of the *Online Safety Act* are:

app includes a computer program.

app distribution service means a service that enables end-users to download apps, where the download of the apps is by means of a carriage service.

Finally, a key concept is that of a 'hosting service', which is a service that 'hosts' (provides data storage for) a social media service or relevant electronic service.[60]

The next section of this Report considers examples of statutory definitions of social media and analogous terms in the laws of other countries.

60 *Online Safety Act*, s 17.

Chapter 5: Relevant statutory definitions in other countries

Introduction

This chapter considers the kinds of definitions of 'social media service' or 'platform' and related terms used in the regulatory legislation of other countries.

European Union — The Digital Services Act 2022

The *Digital Services Act 2022* of the European Union[61] defines the terms 'online platform', 'online search engine', 'online interface' and 'intermediary service'. Relevant definitions in the English language version of the Act, include the following:.

> 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this regulation.
>
> 'online search engine' means an intermediary service that allows users to input queries in order to perform searches of in-principle, all websites, or all websites in a particular language on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can bound.

A key term is 'intermediary service', which includes a 'mere conduit' service, a 'caching' service and a 'hosting' service.

The United Kingdom — The Online Safety Act 2023

The *Online Safety Act 2023* (UK) defines the term 'user-to-user service' in s 3 as follows:

> 3 **"User-to-user service" and "search service"**
>
> (1) In this Act 'user-to-user service' means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service.
>
> (2) For the purposes of subsection (1)—

[61] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC* (Digital Services Act).

(a) it does not matter if content is actually shared with another user or users as long as a service has a functionality that allows such sharing;

(b) it does not matter what proportion of content on a serviced is content described in that subsection.

(3) For the meaning of 'content' and 'encounter', see section 236.

(4) In this Act 'search service' means an internet service that is, or includes, a search engine (see section 229).

(5) Subsections (6) and (7) have effect to determine whether an internet service that—

(a) is of a kind described in subsection (1), and

(b) includes a search engine,

Is a user-to-user service or a search service for the purposes of this Act.

(6) It is a search service if the only content described in subsection (1) that is enabled by the service is content of any of the following kinds—

(a) content mentioned in paragraph 1, 2 or 3 of Schedule 1 (emails, SMS and MMS messages, one-to-one live aural communications) and related identifying content;

(b) content arising in connection with any of the activities described in paragraph 4(1) of Schedule 1 (comments etc on provider content);

(c) content present on a part of the service in relation to which the conditions in paragraph 7(2) of Schedule 1 are met (internal business service conditions).

(7) Otherwise, it is a user-to-user service.

The Act, in s 4(2) provides:

(2) A user-to-user service is a 'regulated user-to-user service' and a search service is a 'regulated search service', if the service—

(a) has links with the United Kingdom (see subsections (5) and (6)); and

(b) is not—

(i) a service of a description that is exempt as provided for by Schedule 1, or

(ii) a service of a kind described in Schedule 2 (services combining user-generated content or search content not

regulated by this Act with pornographic content that is regulated).

(4) Regulated service means—

(a) a regulated user-to-user service,

(b) a regulated search service, or

(c) an internet service, other than a regulated user-to-user service or a regulated search service, that is within section 80(2) (including a service of a kind described in Schedule 2).

(5) For the purposes of subsection (2), a user-to-user service or a search service 'has links with the United Kingdom" if—

(a) the service has a significant number of United Kingdom users, or

(b) United Kingdom users form one of the target markets for the service (or the only target market).

(6) For the purposes of subsection (2), a user-to-user service or a search service also 'has links with the United Kingdom' if—

(a) the service is capable of being used in the United Kingdom by individuals, and

(b) there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom presented by—

(i) in the case of a user-to-user service, user-generated content present on the service or (if the service includes a search engine) search content of the service;

(ii) in the case of a search service, search content of the service.

Schedule 1 to the Act describes 'exempt user-to-user' and 'search services'. It covers:

1. Email services

2. SMS and MMS services

3. Services offering only one-to-on e live aural communications

4. Limited functionality services

5. Services which enable combinations of user-generated content

6. Internal business services (entire user-to-user service or search service)

7. Internal business services (part of user-to-user service or search service)

8. Services provided by public bodies

9. Services provided by persons providing education or childcare

The preceding list of exempt services sets a limit on the application of the UK Act. As already observed, where a broad generic definition of 'social media service' or its analogues is used for the purposes of regulation, it is necessary to create a mechanism for identifying species of the genus which, consistently with the legislative policy, it is not intended to cover. This can be done by writing the exempt species into the legislation. However, that is an option pregnant with litigious possibilities. An alternative is to provide a mechanism, by regulation or ministerial determination or other subordinate legislative instrument, to identify services carved out from the generic definition which are not intended to be covered. The exemption would be directed to social media services which provide no or no significant risk of the kind to which the policy underpinning the proposed law is directed. Such exemptions could be designated by way of category of service as above, or by naming of a service or by a combination of both.

Canada — Online Harms Act

Bill C-63, a proposed new *Online Harms Act* was introduced into the Canadian Parliament in February 2024. The proposed *Online Harms Act* would include a definition of 'social media service' as follows:

> *Social media service* means a website or application that is accessible in Canada, the primary purpose of which is to facilitate interprovincial or international online communication among users of the website or application by enabling them to access and share content.

By cl 2(2) the Bill provides:

> **For greater certainty – social media service**
>
> (2) For greater certainty, a social media service includes
>
> **(a)** an adult content service, namely a social media service that is focused on enabling its users to access and share pornographic content; and
>
> **(b)** a live streaming service namely a social media service that is focused on enabling its users to access and share content by live stream.

There are a number of categories of service which are excluded from the definition of 'social media service' in the proposed *Online Harms Act*. Clause 5(1) provides:

> For the purposes of this Act a service is not a social media service if it does not enable a user to communicate content to the public

That is elaborated in cl 5(2):

> **5(2)** For the purposes of subsection (1), a service does not enable a user to communicate content to the public if it does not enable the user to communicate content to a potentially unlimited number of users not determined by the user.

The concept of a 'regulated service' is defined in s 3 of the Bill as follows:

> **Regulated service**
>
> **3(1)** For the purposes of this Act, a regulated service is a social media service that
>
> **(b)** has a number of users that is equal to or greater than the significant number of users provided for by regulations made under subsection (2);
>
> **(c)** has a number of users that is less than the number of users provided for by regulations made under subsection (2) and is designated by regulations made under subsection (3).

There follows, in s 3(2) a power to make regulations:

> **(a)** establishing types of social media services;
>
> **(b)** respecting the number of users referred to in … subsection [1], for each type of social media service; and
>
> **(c)** Respecting the manner of determining the number of users of a social media service.

There is also a power, under s 3(3) to make regulations designating a particular social media service if the Governor in Council is satisfied that there is a significant risk that harmful content is accessible on the service.

The duties imposed under the Act on the operator of a regulated service do not apply in respect of any private messaging feature of the service (cl 6(1). The concept of a 'private messaging feature' is defined in cl 6(2). It means a feature that:

> 6(a) enables a user to communicate content to a limited number of users determined by the user; and
>
> (b) does not enable a user to communicate content to a potentially unlimited number of users not determined by the user.

Singapore — Online Safety (Miscellaneous Amendments) Act 2022 (amending the Broadcasting Act 1994)

The *Online Safety (Miscellaneous Amendments) Act 2022* amended the *Broadcasting Act 1994* and the *Electronic Transactions Act 2010.* The amendments to the *Broadcasting Act 1994* came into operation on 1 February 2023. The *Broadcasting Act 1994* now contains a definition of 'online communication service' and associated terms.

> **2,A.**—(1) In this Act, an online communication service means an electronic service that is, or a part of an electronic service having the characteristics that are, specified in the Fourth Schedule.
>
> (2) For the purposes of subsection (1), an electronic service means a service —
>
> *(a)* that —
>
> (i) enables end-users to access or communicate content on the Internet using that service, including a point-to-multipoint service; or
>
> (ii) delivers content on the Internet to persons having equipment appropriate for receiving that content, where the delivery of the service is by a service described in sub-paragraph (i);
>
> *(b)* that is a service —
>
> (i) between a point in Singapore and one or more other points in Singapore; or
>
> (ii) between a point and one or more other points, where the firstmentioned point is outside Singapore and at least one of the other points is inside Singapore; and
>
> *(c)* that is not an excluded electronic service.

Section 2A(3) sets out excluded electronic services as follows:

> *(a)* an SMS service;
>
> *(b)* an MMS service;
>
> *(c)* an internet access service;
>
> *(d)* an electronic service where the only user-generated content enabled by that service is one-to-one live aural communications;
>
> *(e)* an electronic service where the only user-generated content enabled by that service is communication between 2 or more end-users that is of a private or domestic nature;

(f) an electronic service where the user-generated content enabled by that service is accessible substantially or only to a closed group of end-users employed or engaged in a business (whether or not carried on for profit) and solely for their use as a tool in the conduct of that business; or

(g) an electronic service that is prescribed by the Minister, by order in the *Gazette*, to be an excluded electronic service, after taking into account the functionalities of the service of the user-generated content enabled by that service or both.

It is worth noting that there is also a definition of 'provider' of an online communication service in s 2D of the Singapore Act:

2D.—(1) Subject to this section, in this Act, the provider of an online communication service is the entity that has control over —

(a) who can use the online communication service that is specified in the Fourth Schedule;

(b) the operations of the characteristics of the electronic service that are specified in the Fourth Schedule in respect of the online communication service; or

(c) which content is communicated or provided on the online communication service.

US Legislation

National Science Foundation

A statutory definition of the term 'social media platform' appears in 42 US Code § 1862w (a)(2) which provides for the National Science Foundation to support research into the impact of social media on human trafficking:

Social Media Platform

The term "social media platform" means a website or internet medium that-

(A) permits a person to become a registered user, establish an account, or create a profile for the purpose of allowing users to create, share, and view user generated content through such an account or profile;

(B) enables 1 or more users to generate content that can be viewed by other users of the medium; and

(C) primarily serves as a medium for users to interact with content generated by other users of the medium.[62]

[62] Source: LII Legal Information Institute, ww.law.cornell.edu/uscode/text/42/1862w.

***Kids Off Social Media Act*, S 4213**

The purpose of this Act, which is still pending as a Bill in the US Congress, is:

> To prohibit users who are under age 13 from accessing social media platforms, to prohibit the use of personalized recommendation systems on individuals under age 17, and limit the use of social media in schools.

In the proposed Bill, the term 'social media platform' is defined in s 102(6) as follows:

> (6) SOCIAL MEDIA PLATFORM —
>
> (A) IN GENERAL — The term 'social media platform' means a public-facing website, online service, online application, or mobile application that—
>
> (i) is directed to consumers;
>
> (ii) collects personal data;
>
> (iii) primarily derives revenue from advertising or the sale of personal data; and
>
> (iv) as its primary function provides a community forum for user-generated content, including messages, videos, and audio files among users where such content is primarily intended for viewing, resharing, or platform-enabled distributed social endorsement or comment.
>
> (B) LIMITATION — The term 'social media platform' does not include a platform that, as its primary function for consumers, provides or facilitates any of the following:
>
> (i) The purchase and sale of commercial goods.
>
> (ii) Teleconferencing or videoconferencing services that allow reception and transmission of audio or video signals for real-time communication, provided that the real-time communication is initiated by using a unique link or identifier to facilitate access;
>
> (iii) Crowd-sourced reference guides;
>
> (iv) Cloud storage, file sharing or file collaboration services;
>
> (v) The playing or creation of video games;
>
> (vi) Content that consists primarily of news, sports, sports coverage, entertainment or other information or content that is not user-generated but is preselected by the platform and for which any chat, comment, or interactive functionality is incidental, directly related to, or dependent on the provision of the content provided by the platform;
>
> (vii) Business, product or travel information including user reviews or rankings of such businesses products, or other travel information;

(viii) Educational information, experiences, training, or instruction, including school sanctioned learning management systems;

(ix) An email service;

(x) A wireless messaging service, including such a service provided through short message service or multimedia messaging protocols, that is not a component of, or linked to, a social media platform and where the predominant or exclusive function of the messaging service is direct messaging consisting of the transmission of text, photos, or videos that are sent by electronic means, where messages are transmitted from the sender to the recipient and are not posted publicly or within a social media platform

(xi) A broadband internet access service (Such term is as defined for purposes of section 8.1(b) of title 47, Code of Federal Regulations or any successor regulation);

(xii) A virtual private network or similar service that exists solely to route intern et traffic between locations.

The term 'user' is defined in s 102(8) as follows:

> (8) USER — the term 'user' means, with respect to a social media platform, an individual who registers an account or creates a profile on the social media platform.

This definition of social media platform would appear to include key platforms such as

- X/Twitter
- Facebook
- Instagram
- TikTok
- Snapchat
- YouTube

the definition appears to exclude platforms such as:

- Wikipedia
- Google reviews
- Expedia
- Outlook
- WhatsApp

Kids Online Safety Act, S 1409

This Bill is said to set out requirements to protect minors from online harms. Those requirements apply to cover 'Covered platforms' which must take reasonable measures in the design and operation of products or services used by minors to prevent and mitigate certain harms that may arise from that use, such as sexual exploitation and online bullying. There is a variety of other obligations imposed on Covered platforms.

The term 'Covered platform' is defined very broadly in s 2 and is limited by a long list of exceptions:

> (3) COVERED PLATFORM—
>
> (A) IN GENERAL — The term 'covered platform' means an online platform, online video game, messaging application, or video streaming service that connects to the internet and that is used, or is reasonably likely to be used, by a minor.
>
> (B) EXCEPTIONS — The term 'covered platform' does not include—
>
> (i) an entity acting in its capacity as a provider of—
>
> (I) a common carrier service subject to the Communication Act of 1934 … and all Acts amendatory thereof and supplementary thereto;
>
> (II) a broadband internet access service (as such term is defined for purposes of section 8.1(b) of title 47, Code of Federal Regulations, or any successor regulation);
>
> (III) an email service;
>
> (IV) a teleconferencing or video conferencing service that allows reception and transmission of audio and video signals for real-time communication, provided that—
>
> (aa) is not an online platform, including a social media service or social network; and
>
> (bb) the real-time communication is initiated by using a unique link or identifier to facilitate access; or
>
> (V) a wireless messaging service, including such a service provided through short messaging service or multimedia messaging service protocols, that is not a component or of linked to an online platform and where the predominant or exclusive function is direct messaging consisting of the transmission of text, photos, or videos that are sent by electronic means, where messages are transmitted from the sender to a recipient and are not posted within an online platform or publicly;
>
> (ii) any organization not organized to carry on business for its own profit or that of its members;

(iii) any public or private preschool, elementary, or secondary school, or any institution of vocational, professional, or higher education;

(iv) a library (as defined in section 213(1) of the Library Services and Technology Act (20 U>S.C. 9122(1));

(v) a news website or app where—

(I) the inclusion of video content on the website or app is related to the website or app's own fathering, reporting, or publishing of news content; and

(II) the website or app is not otherwise an online platform;

(v) a product or service that primarily functions as business-to-business software; or

(vii) a virtual private network or similar service that exists solely to route internet traffic between locations.

The term 'online platform' is also defined:

(9) ONLINE PLATFORM — The term 'online platform' means any public-facing website, online service, online application, or mobile application that predominantly provides a community forum for user generated content, such as sharing videos, images, games, audio files, or other content, including a social media serviced, social network, or virtual reality environment.

Arkansas — Act 689 —Social Media Safety Act

The stated purpose of this Act is to require age verification to the use of social media, to clarify liability for failure to perform age verification for use of social media and illegal retention of data and for other purposes.

The term 'social media company' is defined as follows:

(7) (A) 'Social media company' means an online forum that a company makes available for an account to:

(i) Create a public profile, establish an account, or register as a user for the primary purpose of interacting socially with other profiles and accounts;

(ii) Upload or create posts or content;

(iii) View posts or content of other account holders; and

(iv) Interact with other account holders or users, including without limitation establishing mutual connections through request and accept.

(7) (B) 'Social media company' does not include a:

(i) Media company that exclusively offers subscription content in which users follow or subscribe unilaterally and whose platforms' primary purpose is not social interaction;

(ii) Social media company that allows a user to generate short video clips of dancing, voice overs, or other acts of entertainment in which the primary purpose is not educational or informative, does not meet the exclusion under subdivision (7)(B)(i) of this section;

(iii) Media company that exclusively offers interacting gaming, virtual gaming, or an online service, that allows the creation and uploading of content for the purpose of interacting gaming, entertainment, or associated entertainment, and the communication related to that content;

(iv) Company that:

(a) Offers cloud storage services, enterprise cybersecurity services, educational devices, or enterprise collaboration tools for kindergarten through grade twelve (K-12), schools; and

(b) Derives less than twenty-five percent (25%) of the company's revenue from operating a social media platform, including games and advertising; or

(v) Company that provides career development opportunities, including professional networking, job skills, learning certifications, and job posting and application services;

The term 'social media platform' is also defined:

(8) (A) 'Social media platform' means a public or semipublic internet-based service or application:

(i) That has users in Arkansas; and

(ii) (a) On which a substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application.

(b) A service or application that provides email or direct messaging shall not be considered to meet the criteria under subdivision (8)(A)(ii)(a) of this section on the basis of that function alone.

(B) 'Social media platform' does not include an online service, a website, or an application if the predominant or exclusive function is:

(i) Email;

(ii) Direct messaging consisting of messages, photos, or videos that are sent between devices by electronic means if messages are:

(a) Shared between the sender and the recipient or recipients;

(b) Only visible to the sender and the recipient or recipients; and

(c) Are not posted publicly;

(iii) A streaming service that:

(a) Provides only licensed media in a continuous flow from the service, website, or application to the end user; and

(b) Does not obtain a license to the media from a user or account holder by agreement of the streaming service's terms of service;

(iv) News, sports, entertainment, or other content that is preselected by the provider and not use generated, including without limitation if any chat, comment, or interactive functionality that is provided is incidental to, directly related to, or dependent upon provision of the content;

(v) Online shopping or e-commerce, if the interaction with other users or account holders is generally limited to:

(a) The ability to post and comment on review;

(b) The ability to display lists or collections of goods for sale or wish lists; and

(c) Other functions that are focused on online shopping or e-commerce rather than interaction between users or account holders;

(vi) Business-to-business software that is not accessible to the general public;

(vii) Cloud storage;

(viii) Share document collaboration;

(ix) Providing access to or interacting with data visualization platforms, libraries, or hubs;

(x) To permit comments on a digital news website, if the news content is posted only by the provider of the digital news website;

(xi) For the purpose of providing or obtaining technical support for the social media company's social media platform, products, or services;

(xii) Academic or scholarly research;

(xiii) Other research:

(a) If:

(1) The majority of the content is posted or created by the provider of the online service, website, or application; and

(2) The ability to chat, comment, or interact with other users is directly related to the provider's content;

(b) That is a classified advertising service that only permits the sale of goods and prohibits the solicitation of personal services; or

(c) That is used by and under the direction of an educational entity, including without limitation a:

(1) Learning management systems;

(2) Student engagement program; and

(3) Subject-specific or skill-specific program.

(C) 'Social media platform' does not include a social media platform that is controlled by a business entity that has generated less than one hundred million dollars ($100,000,000) in annual gross revenue.

Utah — Social Media Regulation Act

This Act contains a large number of definitions. It defines 'social media platform' thus:

13-63-101 Definitions

As used in this Chapter

(10)

(a) 'Social media platform' means an online forum that a social media company makes available for an account holder to:

(i) create a profile;

(ii) upload posts;

(iii) view the posts of other accountholders; and

(iv) interact with other accountholders or users.

(b) 'Social media platform' does not include an online service, website, or application:

(i) where the predominant or exclusive function is:

(A) electronic mail;

(B) direct messaging consisting of texts, photos, or videos that are sent between devices by electronic means, where messages are:

(i) shared between the sender and the recipient;

(ii) only visible to the sender and the recipient;

(iii) are not posted publicly.

(C) A streaming service that:

(i) provides only licensed media in a continuous flow from the service, website or application to the end user; and

(ii) Does not obtain a license to the media from a user or accountholder by agreement to its terms of service.

(D) news, sports, entertainment or other content that is preselected by the provider and not user generated, and any chat, comment or interactive functionality that is provided incidental to, directly related to, or dependent upon provision of the content;

(E) online shopping or e-commerce, if the interaction with other users or accountholders is generally limited to:

(i) the ability to upload a post and comment on reviews;

(ii) the ability to display lists or collections of goods for sale or wish lists; and

(iii) other functions that are focused on online shopping or e-commerce rather than interaction between users or accountholders.

(F) interactive gaming, virtual gaming, or an online service that allows the creation and uploading of content for the purpose of interactive gaming, edutainment, or associated entertainment and the communication relating to that content.

(G) photo editing that has an associated photo hosting service, if the interaction with other users or accountholders is generally limited to liking or commenting.

(H) a professional creative network for showcasing and discovering artistic content if the content is required to be non-pornographic;

(I) single purpose community groups for public safety if:

(i) The interaction with other users or accountholders is generally limited to that single purpose; and

(ii) The community group has guidelines or policies against illegal content.

(J) providing career development opportunities, including professional networking, job skills, learning certifications and job posting and application services.

(K) business-to-business software;

(L) a teleconferencing or video conferencing service that allows reception and transmission of audio and video signals for real time communication;

(M) Cloud storage;

(N) Shared document collaboration;

(O) cloud computing services which may include cloud storage and shared document collaboration;

(P) providing access to or interaction with data visualization platforms, libraries or hubs;

(Q) to permit comments on a digital news website if the news content is posted only by the provider of the digital news website;

(R) providing or obtaining technical support for a platform product or service;

(S) academic or scholarly research; or

(T) genealogical research; or

(ii) where:

(A) The majority of the content that is posted or created is posted or created by the provider of the online service, website, or application; and

(B) The ability to chat, comment, or interact with other users is directly related to the provider's content.

(iii) that is a classified ad service that only permits the sale of goods and prohibits the solicitation of personal services; or

(iv) that is used by and under the direction of an educational entity including:

(A) a learning management system;

(B) a student engagement program; and

(C) a subject or skills specific program.

It may also be noted that the term 'user' is defined as 'a person who has access to view all, or some of, the posts on a social media platform but is not an accountholder.' That term 'accountholder' is also defined in para (1) under s 13-63-101 as:

> 'Account holder' means a person who has, or opens, an account or profile to use a social media company's platform.

The term 'social media company' is also defined thus:

‘Social media company’ means a person or entity or entity that:

(a) provides a social media platform that has at least 5,000,000 accountholders worldwide; and

(b) is an interactive computer service.

Texas — Securing Children Online through Parental Empowerment (Scope) Act

This Act, in Chapter 509 entitled ‘Use of Digital Services by Minors’ includes relevant definitions as:

Sec. 509.001

(1) ‘Digital service’ means a website, an application, a program, or software that collects or processes personal identifying information with Internet connectivity.

The relevant chapter of the Act limits its application to a digital service provider who provides a digital service that:

(1) Connects users in a manner that allows users to socially interact with other users on the digital service;

(2) Allows a user to create a public or semi-public profile for purposes of signing into and using the digital service; and

(3) Allows a user to create or post content that can be viewed by other users of the digital service, including sharing content on:

(A) a message board;

(B) a chat room; or

(C) a landing page, video channel, or main feed that presents to a user content created and posted by other users.

Nor does the Act apply to:

509.002

(7) an operator or provider regulated by Subchapter D, Chapter 32, Education Code, that primarily provides education services to students or educational institutions;

(8) a person subject to the Family Education Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g) that:

(A) operates a digital service; and

(B) primarily provides education services to students or educational institutions;

(9) a digital service provider's provision of a digital service that facilitates e-mail or direct messaging services, if the digital service facilitates only those services; or

(10) a digital service provider's provision of a digital service that:

(A) primarily functions to provide a user with access to news, sports, commerce, or content primarily generated or selected by the digital service provider; and

(B) allows chat, comment, or other inactive functionality that is incidental to the digital service.

Colorado House Bill 24-1136

This Bill was signed into law in June 2024 and is titled 'Concerning Measures to Encourage Healthier Social Media Use by Youth, and, in Connection Therewith, Making an Appropriation'. Relevantly for present purposes, the term 'social media platform' was defined in the Act as follows:

(4)(a) FOR THE PURPOSES OF THIS SECTION, "SOCIAL MEDIA PLATFORM" MEANS AN INTERNET BASED SERVICE, WEBSITE OR APPLICATION THAT:

(I) HAS MORE THAN ONE HUNDRED THOUSAND ACTIVE USERS IN COLORADO;

(II) PERMITS A PERSON TO BECOME A REGISTERED USER, ESTABLISH AN ACCOUNT, OR CREATE A PUBLIC OR SEMI-PUBLIC PROFILE FOR THE PURPOSE OF ALLOWING USERS TO CREATE, SHARE, AND VIEW USER-GENERATED CONTENT THROUGH THE ACCOUNT OR PROFILE;

(III) ENABLES ONE OR MORE USERS TO CREATE OR POST CONTENT THAT CAN BE VIEWED BY OTHER USERS OF THE MEDIUM; AND

(IV) INCLUDES A SUBSTANTIAL FUNCTION TO ALLOW USERS TO INTERACT SOCIALLY WITH EACH OTHER WITHIN THE SERVICE OR APPLICATION. A SERVICE OR APPLICATION THAT PROVIDES ELECTRONIC MAIL OR DIRECT MESSAGING SERVICES DOES NOT MEET THE CRITERION DESCRIBED IN THIS SUBSECTION (4) ON THE BASIS OF THAT FUNCTION ALONE.

(b) "SOCIAL MEDIA PLATFORM" DOES NOT INCLUDE AN INTERNET-BASED SERVICE OR APPLICATION IN WHICH THE PREDOMINANT OR EXCLUSIVE FUNCTION IS:

(I) PROVIDING ELECTRONIC MAIL;

(II) FACILITATING COMMERCIAL TRANSACTIONS, IF THE INTERACTION WITH OTHER USERS OR ACCOUNT HOLDERS IS GENERALLY LIMITED TO:

(A) THE ABILITY TO UPLOAD A POST AND COMMENT ON REVIEWS OR THE ABILITY TO DISPLAY LISTS OR COLLECTIONS OF GOODS FOR SALE OR WISH LISTS; AND

(B) THE PRIMARY FUNCTION OF THE PLATFORM IS FOCUSED ON ONLINE SHOPPING OR E-COMMERCE RATHER THAN INTERACTIONS BETWEEN USERS OR ACCOUNT HOLDERS;

(III) FACILITATING TELECONFERENCING AND VIDEO CONFERENCING FEATURES THAT ARE LIMITED TO CERTAIN PARTICIPANTS IN THE TELECONFERENCE OR VIDEO CONFERENCE AND ARE NOT POSTED PUBLICLY OR FOR BROAD DISTRIBUTION TO OTHER USERS;

(IV) FACILITATING CROWD-SOURCED CONTENT FOR REFERENCE GUIDES SUCH AS ENCYCLOPEDIAS AND DICTIONARIES;

(V) PROVIDING CLOUD-BASED ELECTRONIC SERVICES, INCLUDING CLOUD-BASED SERVICES THAT ALLOW COLLABORATIVE EDITING BY INVITED USERS;

(VI) CONSISTING PRIMARILY OF NEWS, SPORTS, ENTERTAINMENT, OR OTHER CONTENT THAT IS PRESELECTED BY THE PROVIDER AND NOT USER GENERATED, AND ANY CHAT, COMMENT, OR INTERACTIVE FUNCTIONALITY THAT IS PROVIDED INCIDENTAL TO, DIRECTLY RELATED TO, OR DEPENDENT UPON PROVISION OF THE CONTENT; OR

(VII) INTERACTIVE GAMING, VIRTUAL GAMING, OR AN ONLINE SERVICE THAT ALLOWS THE CREATION AND UPLOADING OF CONTENT FOR THE PURPOSE OF INTERACTIVE OR VIRTUAL GAMING.

(VIII) PROVIDING INFORMATION CONCERNING BUSINESSES, PRODUCTS, OR TRAVEL INFORMATION, INCLUDING USER REVIEWS OR RANKINGS OF BUSINESSES OR PRODUCTS;

(IX) FACILITATING COMMUNICATION WITHIN A BUSINESS OR AN ENTERPRISE AMONG EMPLOYEES OR AFFILIATES OF THE BUSINESS OR ENTERPRISE SO LONG AS ACCESS TO THE SERVICE OR APPLICATION IS RESTRICTED TO EMPLOYEES OR AFFILIATES OF THE BUSINESS OR ENTERPRISE;

(X) SELLING ENTERPRISE SOFTWARE TO BUSINESSES, GOVERNMENTS, OR NONPROFIT ORGANIZATIONS;

(XI) PROVIDING A STREAMING SERVICE THAT STREAMS ONLY LICENSED MEDIA IN A CONTINUOUS FLOW FROM THE SERVICE, WEBSITE, OR APPLICATION TO THE END USER AND DOES NOT REQUIRE A USER OR ACCOUNT HOLDER TO OBTAIN A LICENSE FOR THE MEDIA BY AGREEMENT WITH A SOCIAL MEDIA PLATFORM'S TERMS OF SERVICE;

(XII) PROVIDING AN ONLINE SERVICE, WEBSITE, OR APPLICATION THAT IS USED BY OR UNDER THE DIRECTION OF AN EDUCATIONAL ENTITY, INCLUDING A LEARNING MANAGEMENT

SYSTEM, A STUDENT ENGAGEMENT PROGRAM, OR A SUBJECT- OR SKILL-SPECIFIC PROGRAM, FOR WHICH THE MAJORITY OF THE CONTENT IS CREATED OR POSTED BY THE PROVIDER OF THE ONLINE SERVICE, WEBSITE, OR APPLICATION AND THE ABILITY TO CHAT, COMMENT, OR INTERACT WITH OTHER USERS IS DIRECTLY RELATED TO THE PROVIDER'S CONTENT;

(XIII) PROVIDING OR OBTAINING TECHNICAL SUPPORT FOR A PLATFORM, PRODUCT, OR SERVICE;

(XIV) PROVIDING CAREER DEVELOPMENT OPPORTUNITIES, INCLUDING PROFESSIONAL NETWORKING, JOB SKILLS, LEARNING CERTIFICATIONS, AND JOB POSTING AND APPLICATION SERVICES;

(XV) FOCUSED ON FACILITATING ACADEMIC OR SCHOLARLY RESEARCH; OR

(XVI) REPORTING OR DISSEMINATING NEWS INFORMATION FOR A MASS MEDIUM, AS DEFINED IN SECTION 13-90-119.

Florida Statutes* §501.1736 (2024) — *Online Protection of Minors Act

This Act was approved by Governor on 25 March 2024.

The Act defines 'social media platform' as follows:

(1)(e)'Social media platform' means an online forum, website, or application that satisfies each of the following criteria:

1. Allows users to upload content or view the content or activity of other users;

2. Ten percent or more of the daily active users who are younger than 16 years of age spend on average 2 hours per day or longer on the online forum, website, or application on the days when using the online forum, website, or application during the previous 12 months or, if the online forum, website, or application did not exist during the previous 12 months, during the previous month;

3. Employs algorithms that analyze user data or information on users to select content for users; and

4. Has any of the following addictive features:

a. Infinite scrolling, which means either:

(I) Continuously loading content, or content that loads as the user scrolls down the page without the need to open a separate page; or

(II) Seamless content, or the use of pages with no visible or apparent end or page breaks.

b. Push notifications or alerts sent by the online forum, website, or application to inform a user about specific activities or events related to the user's account.

c. Displays personal interactive metrics that indicate the number of times other users have clicked a button to indicate their reaction to content or have shared or reposted the content.

d. Auto-play video or video that begins to play without the user first clicking on the video or on a play button for that video.

e. Live-streaming or a function that allows a user or advertiser to broadcast live video content in real-time.

The term does not include an online service, website, or application where the exclusive function is e-mail or direct messaging consisting of text, photographs, pictures, images, or videos shared only between the sender and the recipients, without displaying or posting publicly or to other users not specially identified as the recipients by the sender.

The preceding examples do not cover all US States. They are sufficient to demonstrate the desire of legislators in the United States to confine the application of their laws by carving out of the relevant definitions what amount to exempt services or services to which the legislation does not apply.

The State definitions in the United States illustrate the complexities of drafting into a statute an elaborate definition coupled with an array of exceptions, each of which may be the subject of debate about its scope.

Chapter 6: Regulation of social media content and access in Australia

Introduction

This Chapter reviews the current legislative regime in Australia for regulation of social media by the Commonwealth. The purpose of reviewing this legislation is to ensure that any proposed South Australian law regulating children's access to social media is not inconsistent with Commonwealth law and is capable of forming part of a national scheme.

Online Safety Act 2021 (Cth)

The *Online Safety Act* is the major piece of Commonwealth legislation regulating the conduct of social media providers. Its stated objects are set out in s 3 and are:

(a) to improve online safety for Australians; and

(b) to promote online safety for Australians.

Section 4 sets out a simplified outline of the Act which includes the following elements:

- the establishment of an eSafety Commissioner
- the functions of the eSafety Commissioner
- the complaints system for cyber bullying material targeted at an Australian child
- the complaints system for cyber-abuse material targeted at an Australian adult
- the complaints and objections system for non-consensual sharing of intimate images
- the online content scheme
- the determination by the Minister of basic online safety expectations of social media services, relevant electronic services and designated internet services.

A key definition of central relevance in this legal examination, is the term *'social media service'*. That definition and associated relevant definitions have been set out in Chapters 4 and 5 of this Report.

The scheme of the Act includes provision for the issue of removal notices requiring hosting service providers to cease hosting certain material, to remove material, to remove an intimate

image from the service, to cease hosting the image and to remove and cease hosting certain material. There is also provision for link deletion notices requiring the provider of an internet search engine service to cease providing a link to certain material. An app removal notice may require a provider of an app distribution service to cease enabling end-users to download an app that facilitates the posting of certain material on a social media service, relevant electronic service or designated internet service.

The Act allows for the concurrent operation of State and Territory laws on the same subject matter. Section 234 provides:

> **Concurrent operation of State and Territory laws**
>
> It is the intention of the Parliament that this Act is not to apply to the exclusion of a law of a State of Territory to the extent to which that law is capable of operating concurrently with this Act.

The Act establishes the office of the eSafety Commissioner, who has responsibilities including:

- educational and research functions
- administering a complaints system for cyber-bullying material targeted at an Australian child; and
- administering a complaints system for cyber-abuse material targeted at an Australian adult; and
- administering a complaints and objections system for non-consensual sharing of intimate images; and
- powers to require internet service providers to block access to material involving abhorrent violent conduct; and
- administering the 'online content scheme'.[63]

The eSafety Commissioner has powers of investigation, information gathering and enforcement action in relation to complaints and breaches of the Act.

---

63 *Online Safety Act*, s 27.

Complaints systems

Complaints may be made to the eSafety Commissioner by or on behalf of an Australian child who was or is the target of cyber-bullying material on social media (or other online services covered by the *Online Safety Act* including 'relevant electronic services'). Section 6 of the *Online Safety Act* provides that material is cyber-bullying material if it was targeted at an Australian child and an ordinary reasonable person would conclude that:

(i) it is likely that the material was intended to have an effect on a particular Australian child; and

(ii) the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child.

Action against cyber-bullying of a child can be targeted at a range of actors. The end-user who posted the cyber-bullying material can be given a notice ('an end-user notice') requiring the person to do any or all of the following:

(a) take all reasonable steps to ensure the removal of the material;

(b) refrain from posting any cyber-bullying material for which the child is the target;

(c) apologise for posting the material.

Breach of an end-user notice is not a civil penalty provision. However, end-user notices in relation to cyber-bullying of a child can be enforced via injunctions under Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth).

In addition, social media services can be issued with removal notices requiring them to remove cyber-bullying material from their service. A hosting service provider can be required to cease hosting material. Unlike end-user notices, breach of a removal notice is a civil penalty provision (see s 67 of the *Online Safety Act*).

There are also complaints systems for cyber-abuse material targeted at Australian adults and for non-consensual sharing of intimate images.

Abhorrent Violent Conduct — Blocking of access

Part 8 of the *Online Safety Act* creates a regime whereby internet service providers can be required to block access to material that promotes, incites, instructs in or depicts 'abhorrent violent conduct'. Requests or notices for internet service providers to block abhorrent violent

conduct may only be issued if the eSafety Commissioner is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

Online Content Scheme

Part 9 of the *Online Safety Act* sets out the 'Online content scheme' as a means for the eSafety Commissioner to regulate social media platforms and other online service providers within the Australian jurisdiction. The focus of Part 9 is restricting online access to Class 1 and Class 2 material. Class 1 and 2 materials are defined by reference to the *Classification (Publications, Films and Computer Games) Act 1995* and include material that has been, or would be likely to be, given specific high level classifications under that regime, including 'RC' (Refused Classification), Category 1 or 2 Restricted or X-18+. Section 105 provides a simplified outline of Part 9:

> **105 Simplified Outline of this Part**
>
> - The provider of a social media service, relevant electronic service or designated internet service, may be given a notice (*a* ***removal notice***) requiring the provider to remove certain material.
> - A hosting service provider may be given a notice (a ***removal notice*****)** requiring the provider to cease hosting certain material.
> - The provider of an internet search engine service may be given a notice (a ***link deletion notice***) requiring the provider to cease providing a link to certain material.
> - The provider of an app distributions service may be given a notice (an ***app removal notice***) requiring the provider to cease enabling end-users to downland an app that facilitates the posting of certain material on a social media service.
> - Bodies and associations that represents sections of the online industry may develop industry codes.
> - The Commissioner may make an industry standard.
> - The Commissioner may make service provider determinations regulating service providers in the online industry.

Removal, remedial notices, link deletion and app removal notices

The eSafety Commissioner has a range of enforcement mechanisms under the Online Content Scheme, to ensure that relevant material is either not accessible or restricted. Various online service providers can be issued with notices requiring them to take certain actions, the breach

of which can be subject to civil penalty proceedings. Services who receive a notice must comply within 24 hours or such longer period as the eSafety Commissioner allows.

The notices that can be issued by the eSafety Commissioner are Removal Notices, Remedial Notices, Link Deletion Notices and App Removal Notices. It is not necessary for present purposes to expand further upon those measures.

Basic Online Safety Expectations for Social Media — May 2024

Under Part 4 of the *Online Safety Act* the Minister responsible for the Act may, by legislative instrument, determine Basic Online Safety Expectations for social media services provided in Australia (the 'BOSE'). This sits alongside equivalent powers to issue basic safety expectations in relation to other online services. Sections 46 and 47 set out core expectations that must be included in any determination, and the consultation process to be applied before making a determination.

The *Online Safety (Basic Online Safety Expectations) Determination 2022* (the 'BOSE') as amended at May 2024, covers various online services including social media services. Key requirements include:

- taking reasonable steps to proactively minimise material or activity that is unlawful or harmful, and ensuring users can use a service in a safe manner;
- protecting children from content that is not age appropriate like pornography;
- taking reasonable steps to prevent harmful use of anonymous and encrypted services;
- putting in place user-reporting mechanisms, and clearly outlining their terms of service and enforcing penalties for people who breach these terms;
- cooperating with other service providers;
- responding to requests for information from the eSafety Commissioner.

Relevant expectations set out in the BOSE include the following:

> **6. Expectations—provider will take reasonable steps to ensure safe use**
>
> *Core expectation*

(1) The provider of the service will take reasonable steps to ensure that end-users are able to use the service in a safe manner.

…

Additional expectation

(2A) The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children.

Examples of reasonable steps that could be taken

(3) Without limiting subsection (1), (2) and (2A), reasonable steps for the purposes of those subsections could include the following:

(a) developing and implementing processes to detect, moderate, report and remove (as applicable) material or activity on the service that is unlawful or harmful;

(b) if a service or a component of a service (such as online app or game) is likely to be accessed by children (the ***children's service)*** – ensuring that the default privacy and safety settings of the children's service are robust and se to the most restrictive level;

…

(e) ensuring that assessments of safety risks and impacts are undertaken (including child safety risk assessments), identified risks are appropriately mitigated, and safety review processes are implemented, throughout the design, development, deployment and post-deployment stages for the service;

…

A notable feature of the determination is that it requires 'reasonable steps' to be taken. It provides examples of such reasonable steps. This is a mechanism which can be adapted to a South Australian law which requires 'reasonable steps' to discharge a duty to prevent children from gaining access to social media services.

Breach of the BOSE is not in itself subject to sanction, however social media services can be required to report on how they are meeting any or all of the BOSE. The obligation to respond to a reporting requirement is enforceable and backed by civil penalties and other mechanisms. eSafety can also publish statements about the extent to which services are meeting the BOSE.

Regulatory guidance for BOSE — July 2024

In July 2024, the eSafety Commissioner issued the 'Basic Online Safety Expectations: Regulatory Guidance' (the 'Guidance'). The Expectations were said to apply to three main sections of the online industry. The eSafety Commissioner identified those in the following categories:

(1) social media services including but not limited to:

- social networks;
- media sharing networks;
- discussion forums;
- consumer review networks

(2) Relevant electronic services, including but not limited to:

- email services;
- instant messaging services;
- SMS and MMS services;
- chat services;
- online games where end-users can play with or against each other;
- online dating services.

(3) Designated internet services, including but not limited to:

- websites and file/photo storage services and some services which deploy or distribute generative AI models (unless a service is otherwise considered a social media service or a relevant electronic service).

The Guidance pointed to the highlighting in the BOSE of the importance of minimising the extent to which certain materials are available on a provider's service, including:

- cyber-bullying material targeted at an Australian child.

Specific reference was also made to class 2 material, being material that could be harmful for a child to see. Such material would likely be classified as either:

- X 18 + (or in the case of publications Category 2 Restricted)
- R 18 + (or in the case of publications, Category 1 Restricted).

It is pointed out that the Expectations specifically require providers to take reasonable steps to prevent access by children to class 2 material.

The Guidance went on to discuss the 'reasonable steps' a provider should take to comply with the BOSE.

Part 4 of the document was said to '[set] out more detailed guidance for providers on steps that could be taken to comply with the [BOSE] but did not prescribe specific steps for the use of particular technology. This guidance also sets out where certain harms or safety issues are likely to require a more rigorous or particular response to meet the relevant [BOSE].'[64]

The Commissioner observed in the Guidance that what would be 'reasonable' for a provider to do to address unlawful and harmful material under the Expectations may extend beyond the minimum requirement in the mandatory (and enforceable) industry code or industry standard. Additional steps may be required to meet the applicable expectations.

Comment

That approach is open to the South Australian Government, i.e., using guidance on measures which might constitute minimum necessary steps to meet a reasonable steps standard. The identification of minimum necessary steps does not mean that they are sufficient to meet that standard at any given time having regard to available technologies and measures. Alternatively, such measures may be defined as 'sufficient' to meet the reasonable steps standard.

So far as the term 'reasonable' is concerned, the Commissioner observed that it is not defined in the Act or Determination and bears the ordinary meaning based upon or according to reason and capable of sound explanation. What steps would be reasonable would be a question of fact

64 eSafety Commissioner, 'Basic Online Safety Expectations: Regulatory Guidance', July 2024, 8.

in each case — an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. The Commissioner continued:

> What is reasonable can be influenced by current standards and practices, the nature and extent of the harms involved that require mitigation, as well as by other legislative requirements or obligations that apply to each provider.[65]

For the purposes of this Examination, the terminology of 'reasonable steps' in this Act is applicable to measures necessary to satisfy a duty to prevent access to a social media service by children under the age of 14 or without parental consent if between 14 and 16.

The Guidance also covered the prevention of children's access to class 2 materials. The measures that may be necessary to prevent access to such material are relevant to a consideration of what measures are reasonable to prevent access altogether for children within certain age ranges.

In relation to age assurance, the Guidance stated:

> Age assurance is not defined in the Determination, and is an umbrella term which includes both age verification and age estimation solutions:
>
> - Age verification measures determine a person's age to a high level of accuracy and can involve the use of physical or digital government identity documents to establish a person's age.
>
> - Age estimation technologies provide an approximate age to allow or deny access to age-restricted online content or services. Age estimation can involve the use of biometric data, such as a facial scan or voice recording, to infer a person's age or age range.[66]

By identifying 'appropriate age assurance mechanisms' as an example of a reasonable step, providers have a degree of flexibility as to how they protect children and young people from access to class 2 material. The Explanatory Statement to the 2024 Amendment Determination notes that whether an age assurance mechanism is 'appropriate' will depend on relevant factors such as:

- the effectiveness of the age assurance mechanisms;

- the extent to which class 2 material is provided on the service;

---

65 Ibid 25.
66 Ibid 57.

- the likelihood of children accessing the material on the service.[67]

The Commissioner added that age assurance mechanisms may also support compliance with other applicable expectations, for example by:

- ensuring that under age or prohibited end-users are not able to access services (for example many services do not permit children who are under 13 — which relates to the s 6 expectation on ensuring safe use of a service);
- assisting providers in enforcing bear minimum age requirements and terms of use (also relevant to s 14);
- providing an indication to a service that an end-user is of a certain (or approximate) age, which enables high privacy and safety settings to be implemented by default for that end-user, including preventing access or exposure to certain content on a service (also relevant to s 6).

Reference was also made to restricted access systems set out in the *Online Safety (Restricted Access Systems) Declaration 2022* i.e. measures that may be adopted to prevent children and young people from accessing class 2 material on a service although additional steps may be required depending on the nature of the service.

For services deliberately permitting class 2 material as a core part of the service, it was said to be important that 'robust measures' were in place to prevent children and young people under 18 from accessing the service. These measures included;

- clearly communicating to end-users that the service contains class 2 material and is intended for adult access (over 18 years old);
- applying meta-tags to the sites such as the Restricted Adults label to ensure the service or platform is blocked by any filters that may be in place for children on accounts or devices;
- implementing age assurance or age verification mechanisms to prevent access to the service and to prevent account registrations if accounts are required;

---

[67] Explanatory Statement, *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (Cth), 11.

- ensuring that landing pages or first point of contact with a social media service do not contain class 2 material and that this material is placed behind an age-gate.[68]

Industry Codes and Standards

The implementation of industry codes and industry standards at the behest of the eSafety Commission per Division 7 of the Act, is among the mechanisms that specifically facilitate the accountability of social media platforms. Pursuant to s 135(2)(a), providers of *social media services* constitute a section of the online industry to which appropriate codes and standards will be applicable. An extensive and non-exhaustive list of matters about which industry codes and standards may be made is provided in s 138 of the Act:

> **138 Examples of matters that may be dealt with by industry codes and industry standards**
>
> (1) This section sets out examples of matters that may be dealt with by industry codes and industry standards
>
> (2) The applicability of a particular example will depend on which section of the online industry is involved.
>
> (3) The examples are as follows:
>
> (a) procedures for dealing with class 1 material, or class 2 material, provided on a social media service;
>
> …
>
> (f) 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.
>
> …
>
> (l) promoting awareness of the safety issues associated with social media services.
>
> …
>
> (o) procedures to be followed in order to deal with safety issues associated with relevant social media services.
>
> …
>
> (r) giving parents and responsible adults information about how to supervise and control children's access to material provided on social media services.

[68] Regulatory Guidance, above n 67, 58–59.

…

(v) procedures to be followed in order to deal with complaints about class 1 material, or class 2 material, provided on social media services;

…

(y) procedures to be followed in order to deal with reports about class 1 material, or class 2 material, provided on social media services, where the reports are made by or on behalf of end-users of those services;

…

(zc) if:

(i) class 2 material is provided on a social media service; and

(ii) the service is provided from a foreign country; and

(iii) the provider of the service has reasonable grounds to believe that the material is hosted in Australia; procedures to be followed to ensure the Commissioner is notified of the material;

…

(zh) the making and retention of material directed towards the achievement of the objective of ensuring that, in the event that new relevant electronic services are developed that could put at risk the safety of children who are end-users of the services, the Commissioner is informed about the services.

Section 140 outlines the process and procedures associated with registration of an industry code by the eSafety Commissioner. The eSafety Commissioner may request an industry body or association that represents a particular section of the online industry to develop a code under s 141 of the Act.

Social Media Services Online Safety Code — 2023

On 31 March 2023, the eSafety Commissioner registered the 'Social Media Services Online Safety Code (Class 1A and Class 1B Material)' ('**SMS Code**'). The obligations under that Code came into operation on 16 December 2023.

The SMS Code requires all providers of social media services to undertake an assessment of the risk to Australian end-users and to reassess the risk posed upon the implementation of any significant new feature. The SMS Code provides a guidance matrix for the assessment of a

social media service's risk profile. The mandatory and optional minimum compliance measures under the SMS Code are dependent on the relevant profile of risk for a social media service (Tier 1, 2 and 3). Relevantly to this Examination, the minimum compliance measures for Tier 1 and 2 social media services, include that a social media service must:

- take appropriate enforcement action against end-users who violate terms and conditions and community standards (Measure 2);
- terminate a user's account known to be using the account in breach of age restrictions concerning the use of the service by an Australian child (Measure 3);
- ensure they are appropriately resourced with adequate personnel to oversee the safety of the service (Measure 4);
- make clear in its terms and conditions, community standards and/or user policies the minimum age for an Australian end-user to hold an account (Measure 6);
- take reasonable steps to prevent an Australian child that is known to be under the minimum age permitted on the service from holding an account on the service (Measure 6);
- provide clear and accessible information to parents and carers about how to manage an Australian's child's access and exposure to class 1A and class 1B material (Measure 30).[69]

The Guidance for Minimum Compliance with Measure 6 relating to minimum ages for access to classes 1 and 2 social media services, provides indicative 'reasonable steps' a provider could take to ensure an Australian child less than the minimum age is not using its service, being:

> *i) requiring a user to declare their date of birth during the account registration process;*
>
> *ii) implementing age estimation technology to determine a user's age; or*
>
> *iii) using artificial intelligence tools that help to understand someone's real age.*[70]

---

69 *Social Media Services Online Safety Code (Class 1A and Class 1B Material)* ((Industry Code), July 2023).

70 Ibid 11.

The Tier 1 Services are also relevantly required to comply with additional specific minimum compliance measures. A Tier 1 Service that permits an Australian child to hold an account must:

> a) have default settings that are designed to prevent a young Australian child from unwanted contact from unknown end-users, including settings which prevent the location of the child being shared with other accounts by default; and
>
> b) easy to use tools and functionality that can help safeguard the safety of a young Australian child using the service.[71]

Tier 3 Services (with the lowest risk profile) have the lowest number of minimum compliance measures. It was contemplated in the request for registration of the SMS Code that Tier 3 Services could include educational and learning platforms/discussion boards.[72]

Service provider determinations

Under s 151 of the *Online Safety Act*, the eSafety Commissioner may, by legislative instrument, determine rules that apply to various kinds of online service providers, including providers of social media services. The rules must be constitutionally supported in accordance with the requirements of the section.

This power is somewhat similar to the ability to issue an industry standard, as both are enforceable via civil penalty provisions with the same maximum penalty. However, the service provider rules do not mandate the same process as is required to make an industry standard. It does not appear that this power has been used, and further it appears that it currently cannot be used. Section 151(4) provides that the eSafety Commissioner may only make service provider rules relating to matters specified in the legislative rules, and it does not appear any such legislative rules have been made.

Federal Court orders

On application by the eSafety Commissioner, online service providers, including social media services, who have breached civil penalty provisions on two or more occasions may be ordered by the Federal Court to cease providing services.

---

71 Ibid.

72 *Request for Registration of Online Safety Codes* (31 March 2023), 13.

eSafety Commissioner educational and research functions

Under s 27 of the *Online Safety Act*, the eSafety Commissioner has a range of functions related to educating the public about online safety issues and promoting safe use of online services, including:

> (b) to promote online safety for Australians; and
>
> (c) to support and encourage the implementation of measures to improve online safety for Australians; and
>
> …
>
> (e) to collect, analyse, interpret and disseminate information relating to online safety for Australians; and
>
> (f) to support, encourage, conduct, accredit and evaluate educational, promotional and community awareness programs that are relevant to online safety for Australians; and
>
> (g) to make, on behalf of the Commonwealth, grants of financial assistance in relation to online safety for Australians; and
>
> (h) to support, encourage, conduct and evaluate research about online safety for Australians; and
>
> (i) to publish (whether on the internet or otherwise) reports and papers relating to online safety for Australians; and
>
> (j) to give the Minister reports about online safety for Australians; and
>
> (k) to advise the Minister about online safety for Australians; and
>
> (l) to consult and cooperate with other persons, organisations and governments on online safety for Australians; and
>
> (m) to advise and assist persons in relation to their obligations under [the Online Safety Act]
>
> …

The *Telecommunications Act 1997*

The *Telecommunications Act 1997* (Cth) (the '***Telecommunications Act***') was enacted by the federal Parliament under its constitutional power to legislate in respect of posts, telegraphs, and other like services.[73] The *Telecommunications Act* primarily regulates carriers (the owners of telecommunications infrastructure called 'network units')[74] and carriage service providers

---

73 *Constitution* s 51(v).

74 *Telecommunications Act,* s 5.

(those who provide communication services using third party network units, such as an internet service provider).[75] This includes providers of internet telecommunications services. The term 'internet service providers' has the same meaning as in the *Online Safety Act*.

The *Telecommunications Act* has extra-territorial application.[76] It also applies to offshore areas of each of the States and eligible Territories.[77] The term 'content service' is defined in s 15 and includes:

> (c) an online-entertainment service (for example, a video – on – demand service or an interactive computer game service); or
>
> (d) any other on-line service…[78]

The Minister may be legislative instrument specify a service as a content service.[79]

The concept of a person's 'immediate circle' is introduced in s 23 of the *Telecommunications Act*. The 'immediate circle' of a tertiary education institution includes students of the institution.[80]

Carriage service providers can be required to block access to particular online services under s 313(3) of the *Telecommunications Act*, however this is only used in relation to preventing serious criminal offences or threats to national security (see the 'Guidelines for the use of s 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services' issued by the Department of Communications and the Arts).

Under s 99 of the *Telecommunications Act*, specified carriage service providers and/or content service providers can be made subject to rules made by the Australian Communications and Media Authority ('**ACMA**') via a 'service provider determination'. However, this can only be made on topics prescribed by the Regulations or in relation to the provision of carriage services during periods of disaster. The Regulations do not currently prescribe any topics related to social media services. It may be within the power of the federal Government to use the Regulations to empower ACMA to make determinations in relation to social media services if they were found to be a 'content service provider' within the meaning of the

---

75 *Telecommunications Act,* ss 5, 7 and 87.
76 *Telecommunications Act*, s 9.
77 *Telecommunications Act*, s 11(1).
78 Excluding an educational service provided by a State or Territory government.
79 *Telecommunications Act* ss 15(1)(e) and 15(2).
80 *Telecommunications Act*, s 23(1)(m).

Telecommunications Act. However, given more recently created powers under the *Online Safety Act* it is unlikely social media safety issues would be addressed under the *Telecommunications Act*.

***Broadcasting Services Act 1992* (Cth)**

The *Broadcasting Services Act 1992* (Cth) (the '***Broadcasting Services Act***'), Schedule 8 provides for online content services with a legislative scheme of coverage and exemption which is helpful in considering the form of defined coverage under proposed South Australian legislation.

Under the *Broadcasting Services Act,* Schedule 8 'online content services' are regulated in summary as follows:

- The ACMA may make online content service provider rules about gambling promotional content provided on an online content service in conjunction with live coverage of a sporting event.
- The ACMA may exempt an online content service, or an online content service provider, from the online content service provider rules.
- If an online content service provider contravenes the online content service provider rules, the provider may become liable to pay a civil penalty.
- The ACMA may give a remedial direction to an online content service provider if the provider contravenes the online content service provider rules.[81]

The term 'online content service' is defined as:

> **3. Online content service**
>
> …
>
> (a) a service that delivers content to persons having equipment appropriate for receiving that content, where the delivery of the service is by means of an internet carriage service; or
>
> (b) a service that allows end-users to access content using an internet carriage service;

[81] *Broadcasting Services Act 1992* (Cth) sch 8, cl 1.

where the service:

(c) is provided to the public (whether on payment of a fee or otherwise); and

(d) has a geographical link to Australia.

There follows a list of exempt services not included in the definition. A number of these services are mentioned in Schedule 7 to the Act. They include Parliamentary, court and official inquiry services, services which enable end-users to communicate by means of voice calls, voice calls, video calls, emails or instant messaging with other end-users. They extend to SMS and MMS services. They also include, in cl 3(r), a service determined under sub-cl (2).

Sub-clause 3(2) provides that:

> The ACMA may, by legislative instrument, determine one or more services for the purposes of paragraph (1)(r).

There is also a category of 'exempt online simulcast services'.

The Schedule also defines the concept of 'geographical link to Australia' as follows:

> **5 Geographical link to Australia**
>
> (1) For the purposes of this Schedule, a service has a ***geographical link to Australia*** if an ordinary reasonable person would conclude that:
>
> (a) the service is targeted at individuals who are physically present in Australia; or
>
> (b) any of the content provided on the service is likely to appeal to the public, or a section of the public, in Australia.
>
> (2) For the purposes of this clause, content is ***provided on*** a service if the content is:
>
> (a) delivered by the service; or
>
> (b) accessible to end-users using the service.

Clause 6 deals with the concept of an 'online content service provider' thus:

> **6 Online content service provider**
>
> (1) For the purposes of this Schedule, a person does not provide an online content service merely because the person supplies an internet carriage service that enables content to be delivered or accessed.
>
> (2) For the purposes of this Schedule, a person does not provide an online content service merely because the person provides a billing service, or a fee collection service, in relation to an online content service.

The concept of 'provision' of content on an online content service is set out in cl 7:

> **7 When content is provided on an online content service**
>
> (1) For the purposes of this Schedule, content is ***provided on*** an online content service if the content is:
>
> (a) delivered by the online content service; or
>
> (b) accessible to end-users using the online content service.
>
> (2) For the purposes of this Schedule, content is ***provided on*** an online content service to an end-user if the content is:
>
> (a) delivered to the end-user by the online content service; or
>
> (b) accessible to the end-user using the online content service.

The concept of a service provided to the public is defined by the requirement that 'the service is provided to at least one person outside the immediate circle of the person who provides the service.'[82] The term 'immediate circle' has the same meaning as in the *Telecommunications Act 1997*. The term 'internet carriage service' has the same meaning as in the *Online Safety Act*.

The definition of the concept of a 'geographical link to Australia' is of relevance to the limitation of any South Australian legislation to a law that has a territorial connection with South Australia.

Privacy Act 1988 **(Cth)**

The *Privacy Act 1988* (Cth) (the '***Privacy Act***') is the primary legislation by which Australia ensures the protection of people's privacy, particularly in the data driven technological landscape. It has relevance for detection of privacy in relation to personal data provided by individuals using social media and information relating to their usage.

Privacy is not expressly provided for in the *Constitution* as a subject matter over which the Commonwealth government may legislate. The Act was implemented in reliance of the Australian Parliament's express power to make laws with respect to 'external affairs' pursuant to s 51(xxix). The preamble of the Act stipulates that this legislation, at least in part, consolidates Australia's obligations under the *International Covenant on Civil and Political*

[82] *Broadcasting Services Act,* cl 8.

Rights. In relation to State and Territory laws dealing with privacy issues, s 3 of the Commonwealth Act states:

> It is the intention of the Parliament that this Act is not to affect the operation of law of State or a Territory that makes provision with respect to the collection, holding, use, correction or disclosure of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act.

This has the effect that absent a direct conflict between a provision of a State or Territory and the Commonwealth law there will be no indirect inconsistency arising out of the fact the State or Territory law covers subject matter dealt with by the Commonwealth law.

Objects and Applicability of the Privacy Act

So far as it relates to the regulation of social media entities, the *Privacy Act* applies to APP entities, namely Australian Government agencies and private sector organisations within the meaning of ss 6, 6C and 6D respectively. Section 6C provides:

> (1) In this Act:
>
> ***organisation*** means:
>
> (a) an individual; or
>
> (b) a body corporate; or
>
> (c) a partnership; or
>
> (d) any other unincorporated association; or
>
> (e) a trust
>
> that is not a small business, a registered political party, an agency, a State or Territory or a prescribed instrumentality of a State or Territory.

Section 6D provides that a business will be considered a *small business* where their annual turnover for the previous financial year was $3 000 000 or less. Many social media platforms will fall within the meaning of an organisation categorised as an APP entity, for purposes of the obligations prescribed.

Obligations pursuant to the Privacy Act

The Act is predominantly concerned with the regulation of entities that handle personal information, defined by s 6 of the Act as:

> Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

Part III, Division 2 of the Act prescribes binding Australian Privacy Principles ('APP') which cumulatively apply to all APP entities and must not be breached pursuant to s 15. Schedule 1 of the Act separates the principles into five parts, specifically:

> Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.
>
> Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.
>
> Part 3 sets out principles about the APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.
>
> Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.
>
> Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

The APP and associated obligations, as it relates to the collection, holding, use, disclosure, destruction and de-identification of personal information, are as follows:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers

10. Quality of personal information

11. Security of personal information

12. Access to personal information

13. Correction of personal information

Pursuant to Part 3IIB of the *Privacy Act*, specific APP codes may be created at the initiative of the APP entity or at the request of the Information Commissioner.

Section 26A provides that an APP entity 'must not do an act, or engage in a practice, that breaches a registered APP code that binds the entity'.

Review of Privacy Act and implications for regulation of social media

A review of the *Privacy Act* was issued by the Government following the Australian Competition and Consumer Commission's 2019 Digital Platforms Inquiry Final Report. The Review commenced in October 2020, with an Issues Paper followed by a Discussion Paper in 2021. The Review Report highlighted the vulnerability of personal information in the digital age. Specific provisions of the protection of children were proposed — defining a child as an individual who has not reached 18 years of age.

It was proposed that existing guidance on children and young people and their capacity provided by the Office of the Australian Information Commissioner, should continue to be relied upon by APP entities. Entities must decide if an individual under the age of 18 had the capacity to consent on a case-by-case basis. If that were not practical an entity might assume an individual over the age of 15 has capacity unless there is something to suggest otherwise. It was proposed that the Act codify the principle that valid consent must be given with capacity. It would only be reasonable to expect that an individual to whom the APP's entities activities were directed would understand the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting. Proposal 16.5 was as follows:

> Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate

> Design Code, including its exemptions for certain entities including preventative or counselling services.[83]

In the Government Response to the Privacy Act Review, it dealt specifically with the question of children's privacy. The Response referred to the particular vulnerability of children to online harms and their increasing reliance on online platforms, social media, mobile applications and other Internet connected devices in their everyday lives. It was stated:

> While these services provide many benefits to children and young people, there is concern that children are increasingly being 'datafied', with thousands of data points being collected about them, including information about their activities, location, gender, interests, hobbies, moods, mental health and relationship status.[84]

The 2023 ACAP Survey Results showed that protecting their child's privacy is a major concern for 79% of Australian parents and the privacy of their children's personal information is of high importance to 91% of parents when deciding to provide their child with access to digital services.[85]

The Government agreed with the proposed definition of a child as an individual who has not reached 18 years of age. It also agreed in principle with a suite of proposed additional protections to apply specifically to children, including that targeting to a child should be prohibited with an exception for targeting that is in the best interests of the child. The Response went on:

> This proposal recognises that a child's right to participate online should not be unduly limited, and there may be some circumstances where targeting is beneficial for children.[86]

The Government also agreed in principle that trading in the personal information of children should be prohibited. It also agreed in principle that direct marketing to persons under 18 should be prohibited unless the personal information was collected directly from the child and the direct marketing was in the child's best interest.

---

83 Commonwealth of Australia, *Government Response Privacy Act Review Report'*,(Report, September 2023) 30.

84 Commonwealth of Australia, above n 83, 13.

85 Australian Community Attitudes to Privacy Survey 2023, *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023#:~:text=There%20was%20an%20increase%20in,what%20to%20do%20about%20it.>.

86 Commonwealth of Australia, above n 83, 13.

The Government agreed that a Children's Online Privacy Code should be developed as soon as legislative protections for children were enacted to enable the development of such a Code. That Code would apply to online services likely to be accessed by children. It should align with international approaches including the UK Age Appropriate Design Code, with similar exemptions for particular entities such as counselling services.

The Government also supported the proposition that entities should continue to rely on existing OAIC guidance on children and young people and capacity. The Government agreed in principle that the *Privacy Act* should codify the principle that valid consent must be given with capacity.

The Response also stated that:

> To meet requirements in relation to children, it is expected that entities will 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. Age assurance is an umbrella term which includes both age verification and age estimation solutions. Age verification measures determine a person's age to a high level of certainty, while age estimation technologies provide an approximate age or age range.[87]

The term 'reasonable steps' is familiar terminology when defining the limits of regulatory obligations.

Commonwealth and State criminal law relevant to users of social media

Users of social media may be found guilty of crimes for content that they transmit through the service. Part 10.6 of the Commonwealth Criminal Code contains various offences of unlawful uses of carriage services, which would include social media as this is transmitted via internet carriage services. Such offences include using a carriage service to:

- make a threat to kill or cause serious harm (s 474.15);
- make a hoax threat of the presence of an explosive device or other dangerous thing or substance (s 474.16);
- menace, harass or cause offence (s 474.17), with an aggravated version of the offence if the conduct involves the transmission of private sexual material (s 474.17A)
- access, transmit or publish suicide related material (s 424.29A);

87 Commonwealth of Australia, above n 83, 14.

- accessing, transmitting, publishing, distributing, advertising or promoting violent extremist material (s 474.45B);
- various offences involving use of a carriage service in relation to child sexual abuse material (Part 10.6, subdivision D).

In some cases, providers of social media services may be found criminally liable for use of their service by third parties. Criminal offences under South Australian and federal law hold online services responsible if they are aware that their service can be used to access child abuse material, and they fail to take appropriate action.

Section 474.25 of the Criminal Code provides that:

> A person commits an offence if the person:
>
> (a) is an internet service provider or an Australian hosting service provider; and
>
> (b) is aware that the service provided by the person can be used to access particular material that the person has reasonable grounds to believe is child abuse material; and
>
> (c) does not refer details of the material to the Australian Federal Police within a reasonable time after becoming aware of the existence of the material.
>
> Penalty: 800 penalty units.

Section 63AB of the *Criminal Law Consolidation Act 1935* (SA) provides:

> **63AB – Offences relating to Websites**
>
> (1) A person commits an offence if—
>
> (a) the person hosts or administers, or assists in the hosting or administration of, a website; and
>
> (b) the website is used by another person to deal with child exploitation material; and
>
> (c) the person—
>
> (i) intends that the website be used by another person to deal with child exploitation material; or
>
> (ii) is aware that the website is being used by another person to deal with child exploitation material.
>
> Maximum penalty: Imprisonment for 10 years.

(2) It is a defence to a charge of an offence against subsection (1) to prove that the person, on becoming aware that the website was being used, or had been used, by another person to deal with child exploitation material, took all reasonable steps, in the circumstances, to prevent any person from being able to use the website to deal with child exploitation material.

(3) In determining whether a person has taken all reasonable steps, in the circumstances, for the purposes of subsection (2), regard must be had as to whether the person, as soon as it was reasonably practicable, did any of the following:

(a) shut the website down;

(b) modified the operation of the website so that it could not be used to deal with child exploitation material;

(c) notified a police officer that the website was being, or had been, used to deal with child exploitation material, and complied with any reasonable directions given by a police officer as to action to be taken by the person in relation to that use of the website;

(d) notified a relevant industry regulatory authority that the website was being, or had been, used to deal with child exploitation material, and complied with any reasonable directions given by the authority as to action to be taken by the person in relation to that use of the website.

In addition, s 474.34 of the Criminal Code holds 'content services' (which includes social media services within the meaning of the *Online Safety Act*) criminally liable if they are aware that the service can be used to access abhorrent violent material from within Australia and they do not ensure the expeditious removal of the material from the content service.

Defamation

Any person involved in the publication of defamatory material can potentially be held liable for the defamation. In relation to social media publications, this can involve parties at various levels including:

1. The end-user who authored and/or posted the content.

2. An end-user who 'shares' the content.

3. An end-user who made a post or page on which the defamatory content was posted.[88] or

4. The social media platform.

[88] See e.g. *Fairfax Media Publications Pty Ltd v Voller* (2021) 273 CLR 346.

Recently, the Standing Council of Attorneys-General considered and agreed by majority to reforms that would clarify the liability of online actors who publish content as a 'digital intermediary' (being any party involved in a digital publication who was not the author, originator or poster of the matter; see examples 2–4 above). A new defence was added to the national Model Defamation Provisions[89] providing that digital intermediaries are not liable for defamatory content published by third parties using their service unless:

- They have an accessible complaints mechanism; and
- The plaintiff submitted a written complaint to the digital intermediary about the allegedly defamatory material; and
- The digital intermediary failed to take reasonable steps to prevent access to the allegedly defamatory material within 7 days of receiving the complaint.

However, the South Australian Attorney-General did not agree to these reforms (see the Standing Council of Attorneys-General Communique, 22 September 2023). Therefore, whilst other jurisdictions will eventually adopt these reforms in line with the national model laws, South Australia will remain under the current laws in relation to the liability of digital intermediaries for defamatory content. This will mean that in South Australia social media services remain prima facie liable as publishers of defamatory content and will have to rely on existing defences such as qualified privilege, honest opinion or innocent dissemination.

General Observation

The regulation of social media at the Commonwealth level may broadly be said to be focused on content regulation with particular protections in relation to children. Those protections bring in the concept of 'reasonable steps' necessary to meet the requirements of the legislation or standards made under the legislation. The concept of 'reasonable steps' is plainly applicable to general restrictions on access to social media for children within a given age range or range in which parental consent is required. The experience of the eSafety Commissioner and her office in regulation with respect to age assurance mechanisms will be invaluable in providing guidance on what might constitute 'reasonable steps' under a South Australian law.

89 Model Defamation Amendment (Digital Intermediaries) Provisions 2023 (22 September 2023).

Chapter 7: Regulation of child access to social media in other countries

Overview

International legislation before 2022 was directed to the protection of children's data online. Since that time, a number of countries have passed national laws for the protection of children online by restriction or on design and content. These have included France, Germany, Canada, India, South Korea and Japan. The laws so enacted have provided for age verification to protect against exposure to harmful content, requirements for parental consent, limits on internet usage and protections for children's data privacy.

In a very helpful Issues Paper published in April 2024 for the purposes of the statutory review of the *Online Safety Act* conducted by Delia Rickard PSM, a general observation about the global regulatory environment was made:

> While Australia has been a world leader in online safety regulation, the global regulatory environment is rapidly evolving, with newer regulatory schemes focusing on systemic protections, rather than episode-based interventions for particular types of online content. A variety of regulatory approaches exist internationally with countries tending to take either a content and individual complaint-based approach (like Fiji) or a broader systemic approach such as the EU and UK which focus on systems and processes. Some governments (including in Australia and the Republic of Korea), have taken a hybrid approach, with the ability for individuals to make complaints about specific types of online content, as well as placing systemic requirements on digital platforms. Canada has also proposed a hybrid model under its draft Online Harms Act, and Ireland has indicated it may move to a hybrid model in the future.[90]

The European Union passed its *Digital Services Act* in 2022. That Act took effect on 1 January 2024. It applies to illegal and harmful online content and disinformation. It requires internet intermediaries to prevent exposure to age-inappropriate content. It requires them to control and verify access to information by children and to establish grievance reporting channels.

In 2023, the UK enacted the *Online Safety Act* ('**OSA**') which imposed duties of care on user-to-user and search services to identify, mitigate and manage the risks of harm from illegal content and content and activity that is harmful to children. The regulator is the Office of Communications ('**OFCOM**'). Internet platform services are required to be 'safe by design'. They must maintain a 'higher standard of protection' for children than for adults. They must remove illegal content and legal content harmful to children. Services carrying age-

90 Australian Government, *Statutory Review of the Online Safety Act 2021: Issues Paper* (April 2024) 37.

inappropriate content must implement age verification measures. They must regularly conduct and publish 'children's risk assessments'.

An important piece of legislation proposed at the federal level in the United States is the *Kids Online Safety Act* ('**KOSA**'). It had bipartisan support in Congress and was in the Senate legislative calendar as at April 2024. Its important features are a duty of care, the establishment of a set of safeguards for minors, parental tools, and identifying which users are youth. It is evidently supported by a wide coalition of civil society and industry supporters. There is concern from some LGBTQ+ and civil liberty bodies such as the American Civil Liberties Union, about its effects on First Amendment rights. It has been "deeply influenced' by the UK's OSA, albeit it identifies more harms requiring regulation. These include:

- Opioid markets
- Content uploaded from prisons
- Terrorist propaganda
- Disinformation
- Manipulation by AI
- Abuse of public figures

The duty of care is common to the OSA and the KOSA. As used in the OSA, it was derived from the *Health and Safety at Work Act 1974* (UK). This derivation was based upon an analogy between digital platforms and quasi-public places such as offices, bars and theme parks.

A comment of relevance to the present Examination related to the 'statutory duty of care approach' was made in the Issues Paper in April 2024:

> A statutory duty of care approach places duties on the entities who control and are responsible for a hazardous environment to achieve a desired outcome (harm prevention). This places a regulatory burden on the entity controlling the regulated environment, and can increase a regulated framework's capacity to adapt to unique features and changes in the environment.[91]

Thus, a statutory duty of care would include an overarching obligation to exercise care in relation to user harm (including through risk assessments and implementing mitigation

[91] Australian Government, above n 90, 37.

measures). There would also be an obligation to continually assess the effectiveness of those measures. The duties would be enforceable and penalties could apply for failure to comply.

Legislation along the lines of KOSA has been proposed or enacted in a majority of States in the United States, directed at children's use of social media and providing for age verification. Thirty-five States and Puerto Rico have considered laws to protect children using the internet. Twelve States have passed Bills and Resolutions.

The European Union

EU General Law

General Data Protection Regulation

The General Data Protection Regulation of the European Union ('**GDPR**') is a wide-reaching privacy law that protects all residents of the European Union. Under the GDPR, processing of personal data is only lawful on one of six bases, one of which is consent. The GDPR then sets a 'digital age of consent' of 16 years old, under which consent cannot be used as a legal basis for the processing of personal data by an 'information society service'. An information society service is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'

The GDPR further provides that information society services may process the data of children aged 13, 14 and 15 based on consent if allowed under the law of the relevant member country and if consent is also given by a parent. This allows individual Member States to lower the age of digital consent below 16 if they see fit. If the consent of a parent or guardian is relied upon, the GDPR requires information society services to 'make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into account available technology'.[92]

It should be noted that under the GDPR other bases may justify the processing of data of children under the minimum age; the minimum age only applies to processing data based on consent of the data subject.

---

92 *Regulations (EU) 2016/679 of the European Parliament and of the Council* at 27/4/2016, Art 8(2).

As a Regulation of the EU Parliament, the GDPR applies automatically to all EU Member States without the need for local adoption by individual countries.

The GDPR does not require nor prohibit age assurance or age verification methods. However, the data privacy implications of using age verification technologies appears to be an issue of ongoing concern under the GDPR (which will be covered in more detail in a later briefing on age assurance).

Digital Services Act[93]

Article 28 of the *Digital Services Act* of the European Union provides for the online protection of minors, as follows:

> 1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.
>
> 2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.
>
> 3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.
>
> 4. The Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1.

Article 28(3) does not require routine age verification in all cases, although age verification may be one method by which providers ensure 'appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service'.

Most notably, under Article 28 providers are prohibited from conducting targeted advertising on minors based on profiling of data held about the minors. However, this does not appear to prohibit targeted content curation generally (i.e. that is not paid advertising).

The *Digital Services Act* is very new — it has only applied to certain large online platforms from 31 August 2023, and from all platforms from 17 February 2024. There are still areas of uncertainty about how well it will operate.

---

93 *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022*.

Audio-Visual Media Services Directive[94]

Directives require EU countries to achieve a certain result, but leave them free to choose how to do so (as opposed to Regulations which directly create law that applies to all EU countries automatically). EU countries must adopt measures to incorporate a Directive into national law in order to achieve the objectives set by the Directive.

The EU's Audio-Visual Media Services Directive ('the AVMSD') relates to the provision of audio-visual programming. It was amended in 2018 to cover the provision of video content on online platforms. Sub-section (5) of the Preamble provides that:

> While the aim of Directive 2010/13/EU is not to regulate social media services as such, a social media service should be covered if the provision of programmes and user-generated videos constitutes an essential functionality of that service. The provision of programmes and user-generated videos could be considered to constitute an essential functionality of the social media service if the audiovisual content is not merely ancillary to, or does not constitute a minor part of, the activities of that social media service.

Chapter IXA of the AVMSD applies to 'video sharing platform services', which are defined as:

> (aa) … a service ... where the principal purpose of the service or of a dissociable section thereof or **an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility,** in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing; (emphasis added)

This definition will certainly include social media platforms. For example, Ireland recently published a list of video-sharing platforms designated to be under their jurisdiction, which included:

- Facebook
- Instagram

---

94 *Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services* (Audiovisual Media Services Directive).

- YouTube
- Udemy
- TikTok
- LinkedIn
- X
- Pinterest
- Tumblr
- Reddit

The AVMSD does not create generally applicable rules for video sharing platform services in the EU. Instead, it grants Member States the power to make codes of conduct that apply to video-sharing platform services within their jurisdiction, and sets out comprehensive and complex rules determining which jurisdiction a platform will be considered subject to (such that it appears a service must only comply with the rules in one Member State rather than various conflicting sets of local rules).

Member States have a general discretion in setting standards for video sharing platform services within their jurisdiction. However, Article 28B sets minimum standards that must be included in a code of conduct including that:

> 1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video sharing platform providers under their jurisdiction take appropriate measures to protect:
>
> (a) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1);
>
> ...
>
> 3. For the purposes of paragraphs 1 and 2, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest.

> Member States shall ensure that all video-sharing platform providers under their jurisdiction apply such measures. Those measures shall be practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service that is provided. Those measures shall not lead to any ex-ante control measures or upload-filtering of content which do not comply with Article 15 of Directive 2000/31/EC. For the purposes of the protection of minors, provided for in point (a) of paragraph 1 of this Article, the most harmful content shall be subject to the strictest access control measures.
>
> Those measures shall consist of, as appropriate:
>
> …
>
> (f) **establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;**
>
> …
>
> (h) **providing for parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors;**

Potential EU Reforms

The EU's Better Internet for Kids (BIK+) strategy has proposed the creation 'of a comprehensive EU code of conduct on age-appropriate design, building on the new rules provided in the DSA and in line with the AVMSD and GDPR'.[95] Early work by the EU Commission is underway to develop this strategy.

Further, the EU Commission has established a Task Force on Age Verification. The background of this Task Force is:

> The Commission has set up a task force on age verification with Member States for the implementation of the DSA. The objective is to foster cooperation with national authorities of Member States with expertise in the field to identify best practices and standards in age verification. This cooperation would build on existing measures at national level, including those resulting from the transposition of Directive (EU) 2018/1808 (the Audiovisual Media Services Directive), and would take into account relevant ongoing initiatives, as well as the current state of the art and market practices.[96]

---

95 European Commission, 'A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 11 May 2022, 9.

96 European Commission, News Article, 'Digital Services Act: Task Force on Age Verification, 30 January 2024.

At a second meeting of the Taskforce in March 2024, the concept of an EU Digital Identity Wallet ('EUDI') was canvassed. The need for an harmonised EU approach to age verification was emphasised by Member States. It was proposed that a pilot on a proof of concept on the use of EUDI for age verification should be started.

Ireland

Online Safety and Media Regulation Act 2022

Ireland has passed the *Online Safety and Media Regulation Act 2022*, which adopts their obligations under the AVMSD through amendments to the *Broadcasting Act 2009* (Ireland). Section 139K allows the Irish Coimisiún na Meán (Media Commission) to make codes ('online safety codes'), to be applied to designated online services.

Section 139K(2)–(5) sets out guidance and requirements for making online safety codes.

> (2) An online safety code may make provision with a view to ensuring—
>
> (a) that service providers take appropriate measures to minimise the availability of harmful online content and risks arising from the availability of and exposure to such content,
>
> (b) that service providers take any other measures that are appropriate to protect users of their services from harmful online content,
>
> (c) that service providers take any other measures that are appropriate to provide the protections set out in Article 28b(1)(a), (b) and (c) of the Directive, and
>
> (d) that service providers take any measures in relation to commercial communications on their services that are appropriate to protect the interests of users of their services, and in particular the interests of children.
>
> (3) In the case of video-sharing platform services, the Commission shall exercise its powers under this section with a view to ensuring (without prejudice to any other exercise of those powers in relation to video-sharing platform services) that service providers—
>
> (a) take appropriate measures to provide the protections referred to in subsection (2)(c), including appropriate measures referred to in Article 28b(3) of the Directive,
>
> (b) comply with the requirements set out in Article 9(1) of the Directive with respect to audiovisual commercial communications that are marketed, sold or arranged by them, and
>
> (c) take appropriate measures to comply with the requirements set out in Article 9(1) of the Directive with respect to audiovisual commercial

communications that are not marketed, sold or arranged by them, taking into account the limited control they exercise over those communications.

(4) Without prejudice to subsection (2) an online safety code may provide for:

(a) standards that services must meet, practices that service providers must follow, or measures that service providers must take;

(b) in particular, standards, practices or measures relating to the moderation of content or to how content is delivered on services;

(c) the assessment by service providers of the availability of harmful online content on services, of the risk of it being available, and of the risk posed to users by harmful online content;

(d) the making of reports by service providers to the Commission;

(e) the handling by service providers of communications from users raising complaints or other matters.

(5) Without prejudice to subsection (2) or (4), an online safety code may prohibit or restrict, in accordance with law, the inclusion in programmes or user-generated content of commercial communications relating to foods or beverages considered by the Commission to be the subject of public concern in respect of the general public health interests of children, in particular infant formula, follow-on formula or foods or beverages which contain fat, trans-fatty acids, salts or sugars.

The *Online Safety and Media Regulation Act 2022* also allows the Media Commission to establish processes for the making of a complaint to the Commission on the grounds that harmful online content is available on a designated online service. Such a scheme can only be established if there is a relevant online safety code applicable to the relevant designated online services. The Media Commission is currently (as of June 2024) consulting on a draft Online Safety Code.[97]

United Kingdom

Online Safety Act 2023

A useful overview of the *Online Safety Act 2023* (UK) is provided in the Discussion Paper issued as part of the current review of Australia's *Online Safety Act 2021*. That overview states:

> The UK imposes multiple duties on providers of regulated services to identify, mitigate and manage the risks of harm from illegal content and activity and content and activity that is harmful to children. Details on how service providers can meet their obligations will be placed in secondary legislation, codes and guidelines. The

[97] https://www.cnam.ie/wp-content/uploads/2024/05/Online-Safety-Code_vFinal.pdf

regulator (the Office of Communications, or 'Ofcom') is responsible for drafting the codes and guidelines.

Duties apply in relation to illegal content and activity, and content and activity harmful to children, but also encompass system design (safe by design, chid safety design, freedom of expression and privacy protections, and service transparency and accountability).

The duties apply to 'providers of regulated services', including:

- **User-to-user platforms** – where users can upload and share content (for example messages, images, videos, comments) that becomes accessible to others. This includes services such as online discussion forums, social media platforms, dating services and online market places.
- **Search services –** search engines that enable users to search numerous websites and databases
- **Services that provide pornographic content**[98]

It is also pointed out in the Issues Paper that the UK Online Safety Act applies to providers based outside the UK if the service has a significant number of UK users, the UK is the target market or the service can include UK users and there are reasonable grounds to belief that UK individuals are at material risk of significant harm.

Part 3 of the UK Act is outlined in s 6 as follows:

> **6 Overview of Part 3**
>
> (1) This Part imposes duties of care on providers of regulated user-to-user services and regulated search services and requires OFCOM to issue codes of practice relating to some of those duties.
>
> (2) Chapter 2 imposes duties of care on providers of regulated user-to-user services in relation to content and activity on their services.
>
> (3) Chapter 3 imposes duties of care on providers of regulated search services in relation to content and activity on their services.
>
> (4) Chapter 4 imposes duties on providers of regulated user-to-user services and regulated search services to assess whether a service is likely to be accessed by children.
>
> (5) Chapter 5 imposes duties on providers of certain regulated user-to-user services and regulated search services relating to fraudulent advertising.

98 Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts *Statutory Review of the Online Safety Act 2021: Issues Paper* (April 2024), 62–63, (footnote omitted).,

(6) Chapter 6 requires OFCOM to issue codes of practice relating to particular duties and explains what effects the codes of practice have.

(7) Chapter 7 is about the interpretation of this Part, and it includes definitions of the following key terms—

… [various terms defined in Chapter 7 are referred to].

Section 12 sets out safety duties protecting children. It is unnecessary to set it out in full, but some key elements of the provision are quoted here:

12 Safety duties protecting children

(1) This section sets out the duties to protect children's online safety which apply in relation to regulated user-to-user services that are likely to be accessed by children (as indicated by the headings)

All services

(2) A duty, in relation to a service, to take or use proportionate measures relating to the design or operation of the service to effectively—

(a) mitigate and manage the risks of harm to children in different age groups, as identified in the most recent children's risk assessment of the service [a cross reference is made here to the preceding section, s 11]

(b) mitigate the impact of harm to children in different age groups presented by content that is harmful to children present on the service.

(3) A duty to operate a service using proportionate systems and processes designed to—

(a) prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children;

(b) protect children in age groups judged to be at risk of harm from other content that is harmful to children (or from a particular kind of such content) from encountering it by means of the service.

(4) The duty set out in subsection (3)(a) requires a provider to use age verification or age estimation (or both) to prevent children of any age from encountering primary priority content that is harmful to children which the provider identifies on the service.

…

(6) If a provider is required by subsection (4) to use age verification or age estimation for the purpose of compliance with the duty set out in subsection (3)(a), the age verification or age estimation must be of

such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child.

…

(11) If a provider takes or uses a measure designed to prevent access to the whole of the service or a part of the service by children under a certain age, a duty to—

(a) include provisions in the terms of service specifying details about the operation of the measure, and

(b) apply those provisions consistently.

Section 13 is an interpretive provision in relation to safety duties protecting children. It provides, inter alia:

13 Safety duties protecting children: Interpretation

(1) In determining what is proportionate for the purposes of section 12, the following factors, in particular, are relevant—

(a) All the findings of the most recent children's risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to children), and

(b) The size and capacity of the provider of as service.

…

(5) The duties set out in section 12 extend only to such parts of a service as it is possible for children to access.

(6) For the purposes of subsection (5), a provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or that part of it.

There are record keeping and review duties in relation to the substantive duties imposed in relation to regulated user-to-user services. These are set out in s 23. Duties of care are also imposed on providers of search services.

Section 35 provides for children's access assessment. In s 35(2) it states that:

> A provider is only entitled to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service of that part of it.

There is provision in s 41 for codes of practice about duties to be prepared and issued by the Regulator OFCOM.

UK Age Appropriate design: a code of practice for online services

The UK Age Appropriate Design Code is issued under the provisions of the *Data Protection Act 2018* (UK). It sets out fifteen standards of age appropriate design, 'which seeks to protect children **within** the digital world, not protect them from it.'[99] The Code targets providers of online products or services that process data likely to be accessed by children. As stated within the code itself:

> This code addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children.[100]

The standards of age-appropriate design are:

1. **Best interests of the child**: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

2. **Data protection impact assessments**: Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing…

3. **Age appropriate application**: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users…

4. **Transparency:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child…

5. **Detrimental use of data:** Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

6. **Policies and community standards:** Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restrictions, behaviour rules and content policies).

7. **Default settings:** Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

8. **Data minimisation:** Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged…

---

99 Information Commissioner's Office, 'Age appropriate design: a code of practice for online services, 17 October 2022 - 2.1.36, 5.

100 Ibid – 2.1.36, 9.

9. **Data sharing:** Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

10. **Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child)…

11. **Parental controls:** If you provide parental controls, give the child age appropriate information about this…

12. **Profiling:** Switch options which use profiling 'off' by default. (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child)…

13. **Nudge techniques:** Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.

14. **Connected toys and devices:** If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.

15. **Online tools:** Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.[101]

Similar provisions have been implemented in other jurisdictions, including Ireland and States of the United States.

Canada — Bill C-63 Online Harms Act

Bill C-63 was introduced into the House of Commons of Canada for a first reading on 26 February 2024. Its stated purpose is, among other things, 'to promote the online safety of persons in Canada, reduce harms caused to persons in Canada as a result of harmful content online and ensure that the operators of social media services in respect of which that Act applies are transparent and account table with respect to their duties under that Act.'

The Act establishes a Digital Safety Commission of Canada, creates the position of Digital Safety Ombudsperson of Canada and establishes the Digital Safety Office of Canada.

The Act imposes on the operators of social media services in respect of which it applies, the following duties:

> **(i)** a duty to act responsibly in respect of the services that they operate, including by implementing measures that are adequate to mitigate the risk that users will be exposed to harmful content on the services and submitting digital safety plans to the Digital Safety Commission of Canada,

101 Ibid 7–8.

> **(ii)** a duty to protect children in respect of the services that they operate by integrating into the services design features that are provided for by regulations,
>
> **(iii)** a duty to make content that sexually victimizes a child or revictimizes a survivor and intimate content communicated without consent inaccessible to persons in Canada in certain circumstances; and
>
> **(iv)** a duty to keep all records that are necessary to determine whether they are complying with their duties under that Act;

There is also provision for the Digital Safety Commission of Canada to accredit persons to conduct research or engage in education advocacy or awareness activities related to the Act for the purposes of enabling those persons to have access to inventories of electronic data and to electronic data of the operators of social media services in respect of which the Act applies.

It also provides that persons in Canada may complain to the Digital Safety Commission of Canada about certain categories of content on a social media service and authorises the Commission to make orders requiring the operators of those services to make that content inaccessible to persons in Canada.

The definition of 'social media service' under the proposed *Online Harms Act* has been set out earlier in this Report. The term 'child' in the Act is defined to mean a person who is under 18 years of age.[102] A number of species of harmful content are identified and defined.

The term 'operator' is defined as follows:

> ***operator*** means a person that, through any means, operates a regulated service

A 'regulated service' refers to a service referred to in subs 3(1) of the Act, a definition set out earlier in this Report.

Part 4 of the proposed Act is entitled 'Duties of Operators of Regulated Services' and sets out a number of the duties referred to. It is convenient to set out the way in which some of those duties are framed.

> **Duty to implement measures**
>
> **55(1)** The operator a regulated service must implement measures that are adequate to mitigate the risk that users of the service will be exposed to harmful content on the service.

---

102 *Online Harms Act*, s 2(1).

Factors

(2) In order to determine whether the measures implemented by the operator are adequate to mitigate the risk that users of the regulated service will be exposed to harmful content on the service, the Commission must take into account the following factors:

(a) the effectiveness of the measures in mitigating the risk;

(b) the size of the service, including the number of users;

(c) the technical and financial capacity of the operator;

(d) whether the measures are designed or implemented in a manner that is discriminatory on the basis of a prohibited ground of discrimination within the meaning of the *Canadian Human Rights Act*; and

(e) any factor provided for by regulations.

No unreasonable or disproportionate limit on expression

(3) Sub section (1) does not require the operator to implement measures that unreasonably or disproportionately limit users' expression on the regulated service.

Measures in regulations

56 The operator of a regulated service must implement any measures that are provided for by regulations to mitigate the risk that users of the service will be exposed to harmful content on the service.

Section 55(2) sets out factors which the Commission must take into account in determining whether measures implemented by an operator are adequate to mitigate the risk. Under s 56 the operator of the regulated service must implement measures provided for by regulations to mitigate the risk. There is provision for user guidelines (s 57); tools to block users (s 58); tools and processes to flag harmful content (s 59). Operators are required under s 62 to submit digital safety plans to the Commission in respect of each regulated service that they operate.

The next general duty is the duty to protect children, expressed in s 64:

Duty to protect children

64 An operator has a duty, in respect of a regulated service that it operates, to protect children by complying with section 65.

Design features

65 An operator must integrate into a regulated service that it operates any design features respecting the protection of children, such as age appropriate design, that are provided for by regulations.

Guidelines

66 The Commission may establish guidelines respecting the protection of children in relation to regulated services and respecting the manner in which the operator of a regulated service may comply with regulations made under paragraph 140(1)(o). The guidelines are established for information purposes only.

There follows a group of sections dealing with the duty to make certain content inaccessible. In summary if the operator of a regulated service identifies on the service, other than as a result of a flag by a user, content that the operator has reasonable grounds to suspect is content that sexually vicitimises a child or revicitimises a survivor or intimate content communicated without consent, the operator:

(a) must make that content inaccessible to all persons in Canada within the period that applies under subsection (2) and continue to make it inaccessible until the operator makes a decision under subsection 69(2); and

(b) must within the period that applies under subsection (2), give notice to the user whom communicated the content on the service that the content has been made inaccessible.

There follow a number of provisions ancillary to that duty.

There are various remedial powers conferred on the Commission in response to complaints about content. These appear in ss 81 to 85. The Commission is empowered to conduct hearings in response to complaints and has an array of information gathering powers. Section 94 of the proposed Act provides for compliance orders:

Compliance Orders

94(1) If the Commission has reasonable grounds to believe that an operator is contravening or has contravened this Act, it may make an order requiring the operator to take, or refrain from taking, any measure to ensure compliance with this Act.

There is an administrative monetary penalties regime for contraventions of the Act or regulations or orders of the Commission or requirements imposed by inspectors. Section 98 provides:

Purpose of penalty

98 The purpose of a penalty is to promote compliance with this Act and not to punish.

There is provision for the issue of what are called ‘Notices of violation’. There is provision for undertakings in s 107:

Undertaking

107(1) A person that, through any means, operates a social media service may, at any time, enter into an undertaking with the Commission or a person authorized to enter into undertakings.

Content

(2) The undertaking

(a) is to set out the act or omission to which it relates;

(b) is to set out the provision at issue;

(c) may contain any conditions that the Commission or authorized person considers appropriate; and

(d) may include a requirement to pay a specified amount.

Comment

As will be apparent from the preceding review, this Act is directed to harmful content, rather than a general age related restriction on access to social media services. It does, however, reflect a recognition that absolute or strict liability provisions are unrealistic. Proportionate mitigating measures are provided for, supported by regulations and regulator generated guidelines. This model is analogous to the 'reasonable steps' model adopted in the DOSE and contemplated in the proposed legislation for South Australia.

Singapore — Online Safety (Miscellaneous Amendments) Act 2022

The above legislation came into effect in February 2023. It amended the *Broadcasting Act 1994* and the *Electronic Transactions Act 2010*. Definitions in the Act have already been referred to. The Act inserts a new Part 10A into the *Broadcasting Act 1994*. That Part is entitled 'Online Communication Service Regulation'. It is content directed. The purpose of the Part is stated in s 45A:

Purpose

45A. The purpose of this Part is to ensure that providers of online communication services to Singapore end-users —

(a) provide a safe online environment for Singapore end-users that promotes responsible online behaviour, deters objectionable online activity and prevents access to harmful content;

(b) place adequate priority on the protection of Singapore end-users who are children of different age groups from exposure to content which may be harmful to them; and

(c) are regulated in a manner that enables public interest considerations to be addressed.

The application of Part, set out in s 45B has a territorial linkage and is expressed as follows:

Application

45B. This Part applies to and in relation to any content that is provided on any online communication service and is accessible by any Singapore end-user … [the balance of the provision is not material for present purposes].

The concept of providing or communicating content is picked up in s 45C(1):

When content is provided or communicated on online communication service

45C.— (1) For the purposes of this Part, content is provided on an online communication service if the content can be accessed by one or more of the end-users using the service.

There is a concept of 'egregious content' which is spelt out in s 45D. This covers a wide range of content, including content of the kind to which the Commonwealth legislation in Australia is directed.

There follows not the statement of a duty, but simply the creation of offences. Section 45E creates the 'offence of not stopping egregious content on online communication service'. Section 45F creates the offence of not stopping access to an online communication service. Section 45G sets up a defence:

Defence

45G. In a prosecution of the person for an offence against section 45E(1) or 45F(1), it is a defence for the person charged to prove, on a balance of probabilities, that —

(a) it was not reasonably practicable to do more than what was in fact done to satisfy the duty in section 45J; and

(b) there was no better practicable means than was in fact used to satisfy the duty in section 45J.

This leads to s 45J which creates a duty to comply, expressed as follows:

Duty to comply

45J.—(1) every provider of an online communication service or an internet access service to whom is given a section 45H direction or section 45I blocking

> direction, has the duty to take all reasonably practicable steps to comply with the direction given to the provider.
>
> (2) No civil or criminal liability is incurred by a provider of an online communication service or an internet access service provider, or an officer, employee or agent of such a provider, for anything done or omitted to be done with reasonable care and in good faith in complying with a section 45H direction or section 45I blocking direction given to the provider.

Comment

While the Singaporean legislation simply creates offences, those offences are linked to non-compliance with directions given by the relevant Authority under the Act relating to disabling access or stopping delivery or communication of content or stopping access by Singapore end-users. The Act creates a duty to comply with such directions, but limits the duty to taking 'all reasonably practicable steps' to comply with the relevant direction.

Any South Australian legislation imposing a duty to deny access to social media services must necessarily, as in other jurisdictions, limit it to what steps are reasonable and practicable to endeavour to comply with such a duty.

United States of America — Federal Law

Section 230 Communications Decency Act (47 U.S.C 230)

In the United States, internet service providers have limited liability for any content generated by third-party users. Section 230(1) of Chapter 47 of the United States Code provides that:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

This significantly limits the extent to which a social media service provider can be found liable for unlawful content published through their platforms (with some exceptions for federal criminal offences or intellectual property law). Section 230(2) provides that:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Combined, these provisions ensure that there is minimal regulation of the general content of social media in the United States. Social media service providers are neither held liable for content published through their service, nor held liable for any decisions to remove content from the service.

Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501)

There are currently no federal, age-based legislative restrictions in the United States to prohibit the use of social media platforms for children outright. Practically, however, a de facto parental consent law is in place. The *Children's Online Privacy Protection Act of 1998* (15 U.S.C. 6501) (**'COPPA'**) imposes strict privacy restrictions on the collection and use of personal data for children under the age of thirteen by any commercial website or online service. The operator of such a website or service may not knowingly collect personal information from a child without 'verifiable parental consent'. Consequently, most social media services officially require users to be at least 13 years old to open an account.

Proposed Federal legislation

It should be noted that any reforms in the United States, either by a State or the Federal Government, are at risk of being held unconstitutional. The First Amendment of the United States Constitution guarantees freedom of speech, and early cases have already held that some restrictions on social media use may violate this clause.[103].

Even if the reforms described below are passed, there is some risk that they may not become operational due to some or all of the reform being ruled unconstitutional. Whilst similar legislation enacted in Australia would be unlikely to be ruled invalid, US laws however may provide some practical drafting examples for operational social media age restrictions.

Kids Off Social Media Act S.4213

On 30 April 2024, 'A bill to prohibit users who are under age 13 from accessing social media platforms, to prohibit the use of personalized recommendation systems on individuals under age 17, and limit the use of social media in schools' (the 'S.4213 Bill') was introduced into

[103] See, e.g., *NetChoice, LLC v Griffin*, Memorandum Opinion and Order granting Motion for Preliminary Injunction, United States District Court, Western District of Arkansas, 31 August 2023)

the United States Congress and referred to the Committee on Commerce, Science, and Transportation.

The S.4213 Bill proposes the following reforms:

- Tying access to certain school funding to requirements that the school enforce a policy of preventing students from accessing social media platforms on any school supported device or network;

- A ban on social media platforms knowingly allowing a child under the age of 13 to create a social media account, and a requirement for a platform to terminate the account of a person they know to be under the age of 13 and delete all the associated personal data;

    - NB "Know or knows" is defined to mean "to have actual knowledge **or knowledge fairly implied on the basis of objective circumstances.**" This does not require social media platforms to verify or estimate the age of users, (which is expressly stated in the Bill) however it is not clear what "knowledge fairly implied on the basis of objective circumstances" would be? Could this include methods by which age can be approximated from a constellation of the user's interactions and interests etc.?

    - It is noted that this reform would not change the status quo much in practice, as it appears to impose similar restrictions as COPPA, and social media platforms typically already have a minimum age of 13 as part of their terms and conditions.

- Prohibit the use of personal data in 'personalized recommendation systems' on any person under from the ages of 13 to 16 ('teens').

The definition of 'social media platform' in the Act has been referred to earlier in this Report in the chapter dealing with statutory definitions of 'social media' and related terms.

Kids Online Safety Act S.1409

Rather than set specific age limits, the *Kids Online Safety Act* — still pending as a Bill — focuses on measures to make social media safer for minors to use. The Bill would require 'covered platforms' to:

- Take reasonable measures in the design and operation of the products or services used by minors to prevent and mitigate certain harms that may arise from that use including certain mental health disorders and suicide, addiction-like behaviours, sexual abuse, promotion of narcotics and predatory or deceptive marketing practices.

- Provide users known to be minors with a range of readily-accessible and easy-to-use safeguards and options, such as preventing other users from viewing the minor's personal data, limiting features such as automatic playing of media or rewards for time spent on the platform, and the ability to opt out of personalised recommendations.

    - These required features must be the default settings for accounts for minors.

- Provide readily-accessible and easy-to-use parental tools in relation to the accounts of minors, including the ability for parents to view and change the privacy and account settings and to view metrics of total time spent on the platform.

- Provide a means to submit reports of harms to a minor, with mandatory timeframes for responding to the report;

- Require covered platforms of a certain size to regularly disclose specified information about usage by minors.

The definition of the term 'covered platform' has been referred to earlier in this Report in the chapter dealing with statutory definitions of 'social media' and related terms.

United States — State based legislative reforms (enacted)

There have been a number of States in the United States which have enacted relevant legislation, some example are outlined here.

Arkansas – Senate Bill 396 – Social Media Safety Act — subject to preliminary injunction by US District Court.

In 2023, Arkansas passed Senate Bill 396 — the *Social Media Safety Act*. The Act required social media companies to verify the ages of all account holders who reside in Arkansas. Arkansans were required to submit age verification documentation before accessing a social media platform. The Act required a 'social media company' as defined, to outsource the age verification process to a third party vendor. A prospective user would have to upload a specific form of identification to the third party vendor's website. Minors would be denied an account and prohibited from accessing social media platforms unless a parent provided express consent. This required proof of the parent's age, identity and relationship to the minor.

The Act, designated 'Act 689' was to come into effect on 1 September 2023. It was challenged in the United States District Court for the Western District of Arkansas. The plaintiff was NetChoice LLC, an internet trade association whose members included Facebook, Instagram, Twitter, TikTok, Swapchat, Pinterest and Nextdoor. NetChoice was supported by the American Civil Liberty Union in an amicus brief.

The plaintiff's motion for a preliminary injunction was granted on 31 August 2023 by a US District Court Judge who 'preliminarily enjoined' the Act pending further disposition of the issue on the merits.[104]

The definition of 'social media company' and 'social media platform' in the Act has been referred to earlier in this Report in the chapter dealing with statutory definitions of social media and related terms.

The law was enjoined on two grounds: first for the vagueness of its language and secondly for offending against the First Amendment protection of freedom of speech. The first ground has

[104] *NetChoice LLC v Tim Griffin, in his Official Capacity as Attorney-General of Arkansas, Case No 5:23-VCV-05105.*

some practical relevance to the drafting of any Australian law. The Judge quoted from a decision of the US Supreme Court in 1968:

> It is essential that legislation aimed at protecting children from allegedly harmful expression—no less than legislation enacted with respect to adults—be clearly drawn and that the standards adopted be reasonably precise so that those who are governed by the law and those that administer it will understand its meaning and application.[105]

There was a failure to adequately define which entities were subject to the requirements of the law. The term 'primary purpose' was not defined, nor were guidelines provided.

The Judge pointed out that while State's expert, Mr Allan, from the Age Verification Providers' Association in the United Kingdom, said Snapchat was a social media agency, the State's Attorney, did not say that. The terms 'substantial function' and 'predominant function' were not defined. It was not clear what a social media company must do to prove parental relationship. What if divorced parents disagreed about consent? The State's expert, Mr Allan, said that the biggest challenge was establishing the parental relationship.

An analogy was advanced of a mall with a minimum age bar in it and other retail outlets. On the State's approach the whole mall would be closed. The State analogy was not persuasive. Experts did not claim that the majority of content on social media is damaging, harmful or obscene.

YouTube, which was not regulated by the Act, was the most popular online activity involving children aged from 3 to 17.[106] The State had selected what it considered the most dangerous platforms for children but based on data from a 2022 Cyber Tipline Report by Electronic Service Providers (ESP) 1, National Centre for Missing or Exploited Children.

Act 689 was said to be not narrowly tailored to target content harmful to minors. By contrast, the main concern of the UK Online Safety Bill was to protect minors from accessing particular content.

---

105 Ibid 31 citing *Interstate Circuit, Inc v City of Dallas* 390 US 676, 689 (1968).

106 OFCOM – Children and Parent's Media Use and Attitudes Report 2022 (30 March 2022).

Colorado House Bill 24-1136

The Colorado House Bill was signed into law in June 2024 and is entitled 'CONCERNING MEASURES TO ENCOURAGE HEALTHIER SOCIAL MEDIA USE BY YOUTH, AND, IN CONNECTION THEREWITH, MAKING AN APPROPRIATION'.

The Bill recited in s 1 that a 'Social Media and Youth Mental Health advisory' issued on 23 May 2023 by the US Surgeon General recognising 'the growing impact of social media on youth mental health and well-being as a significant public health challenge that require[d] immediate awareness and action.' The Act recited that the advisory included recommendations for policy makers to address the issue. It recited that in the United States up to 95% of youth aged 13 to 17 reported using social media platforms and that a third of youth reported using social media 'almost constantly.'[107]

The advisory also reported that a study of youth in the United States aged 12 to 15 found that those who spend three or more hours a day on social media had double the risk of experiencing poor mental health outcomes, including experiencing symptoms of depression and anxiety. A systematic review of 42 studies on the effects of excessive social media use found a consistent relationship between social media use and poor sleep quality, reduced sleep duration, sleep difficulties and depression among youth. Social media sites were designed to maximise user engagement which could encourage excessive social media use and behavioural dysregulation.[108]

The 2020 Comprehensive Health Academic Standards in Colorado were said to include standards for comprehensive health and physical education, among them the importance of identifying and managing the risk and the impacts of modern technology and social media on students' physical and personal wellness.

A number of substantive provisions followed to amend several statutes.

Section 2 of the Act added a provision to 'Colorado Revised Statutes' requiring the creation by the relevant department and the maintenance of a resource bank of existing evidence-based, research-based scholarly articles, promising program materials and curricula pertaining to the mental and physical health impacts of social media use by youth, internet safety and cyber

107 Bill S 1(c).
108 Bill S 1(c)\-(f).

security. The Act further required that the department convene a temporary stakeholder group to assist with the creation and development of a plan for ongoing maintenance of the resource bank by the department. The stakeholder group would identify avenues for informing local education providers, parents, youth and the public about the resource bank. The materials could be used in elementary and secondary schools in the State.

The department was required to convene a temporary stakeholder group to identify the scholarly articles, materials and curricula to be a part of the resource bank. The department, with the assistance of the stakeholder group, was to identify what grade or age group materials were appropriate for and, when possible, when a material could be used for a standard within the Comprehensive Health Education Standards. The department was to collect data on how often the materials and curricula were accessed.

In s 3, Colorado Revised Statutes were amended to include a requirement that:

> The department of education HAS the authority to promote the development and implementation of local comprehensive health education programs and local student wellness programs, INCLUDING PROGRAMS THAT ADDRESS THE MENTAL HEALTH IMPACTS OF SOCIAL MEDIA USE BY YOUTH.

The guidelines developed by the Department of Education pursuant to that section for Grades 6 through 12 were required to 'STRONGLY ENCOURAGE INCLUDING CURRICULUM ON THE MENTAL HEALTH IMPACTS OF SOCIAL MEDIA USE BY YOUTH.'

Section 4 added a new Part to Article 1 of Title 6 of the Colorado Revised Statutes. The new Part 16 was entitled 'PROTECTIONS FOR YOUTH USING SOCIAL MEDIA'. Relevantly, it was in the following terms:

> (1) ON OR AFTER JANUARY 1, 2026, A SOCIAL MEDIA PLATFORM MUST ESTABLISH A FUNCTION THAT EITHER:
>
> (a) MEETS THE CRITERIA IN SUBSECTION (2) OF THIS SECTION AND BE INFORMED BY THE STANDARDS ESTABLISHED IN SUBSECTION (5) OF THIS SECTION; OR
>
> (b) DISPLAYS A POP-UP OR FULL SCREEN NOTIFICATION TO A USER WHO ATTESTS TO BEING UNDER THE AGE OF EIGHTEEN WHEN THE USER:
>
> (I) HAS SPENT ONE CUMULATIVE HOUR ON THE SOCIAL MEDIA PLATFORM DURING A TWENTY-FOUR-HOUR PERIOD; OR
>
> (II) IS ON A SOCIAL MEDIA PLATFORM BETWEEN THE HOURS OF TEN P.M. AND SIX A.M.

There followed requirements for the function established under the preceding section to provide users under the age of 18 with information about their engagement in social media, to understand its impact on the developing brain, and the mental and physical health of young users.

There were technical requirements that the pop-up function must repeat at least every thirty minutes after the initial notification.

The definition of the term ‘social media platform’ has been referred to earlier in this Report in the chapter dealing with statutory definitions.

Florida — Online Protection of Minors Act

The Online Protection of Minors Act was approved by the Governor of Florida on 25 March 2024. Section 5 will come into operation on 1 January 2025.

This Bill prohibits social media platforms from allowing minors under the age of 14 who generally reside in Florida from becoming account holders, and requires them to terminate the accounts of existing account holders found to be younger than 14 years of age.

Further, users aged 14 or 15 may only hold a social media account with the consent of a confirmed parent or guardian, and to terminate the accounts of users found to be 14 or 15 who have not demonstrated consent from a confirmed parent or guardian, or whose parent or guardian requests the termination of the account. A social media platform is required to permanently delete all personal information held by it in relation to a terminated account.

The Act provides an alternative provision in relation to 14 and 15-year-old users, to come into effect if a court prohibits enforcement of the main provisions. The alternative provision would create a straight ban on 14- and 15-year-old users, rather than allowing them with parental consent.

The definition of the term ‘social media platform’ has been referred to earlier in this Report in the chapter dealing with statutory definitions.

The provisions of the Act are enforced by a system of civil damages. Knowing or reckless violations are deemed actionable unfair or restrictive practices. The Florida Department of Legal Affairs may bring an action against a social media platform under Florida’s existing laws

on such practices. In addition, a civil penalty of up to $50,000 per violation plus costs may be collected by the Department. A failure to comply that is considered a 'consistent pattern of knowing or reckless conduct' may give rise to punitive damages against a platform (§ 501.1736 (5), Fla. Stat. (2024)).

The Act also provides that a social media platform that knowingly or recklessly violates §§ 501.1736 (2), (3) or (4), is liable to the minor account holder for up to $10,000.00 in damages and costs. Any action must be brought on behalf of the minor account holder within one year from the date the complainant knew, or ought to have known, of the violation (§§ 01.1736(6)(b) and (c).

In addition to the provisions in § 501.1736, with respect to social media access for children and young people, § 501.1737, provides for mandatory age verification for online access to sites that contain a 'substantial proportion' of materials harmful to minors (sexual content). A 'substantial proportion is defined as 33.3% or more. These age verification provisions are unlikely to apply to typical social media websites.

Other States

Other States of the United States which have enacted legislation in this area include:

Ohio— Parental Notification by Social Media Operators Ohio Act Rev Code ANN S1349.09

Connecticut — Concerning Online Privacy Data and Safety Protections SB 3 No 7.

Louisiana — Secure Online Child Interaction and Age Limitation Act LA Stat Ann § 51.1751-59

Tennessee — Protecting Children from Social Media Act HB 1891.

Georgia — Protecting Georgia's Children on Social Media Act 2024 GA SB 351

Comment

The regulatory models dealing with protection of children in relation to social media services are various. Attractive features include:

(1) A generic definition.

(2) Specification of services not covered — although this is perhaps best done for the most part by regulation or other subordinate legislative instrument.

(3) Imposition of duties of care not to allow access to children in the prohibited age ranges and to take reasonable steps to prevent such access.

Chapter 8: Age Assurance — verification and estimation

Introduction

Any duty imposed on social media service providers to restrict access to their services by reference to the age of users must be capable of compliance. Compliance is only possible to the extent that there are age assurance mechanisms available to providers. The technologies for age assurance are evolving. That evolution has been the subject of public discussion in Australia involving the eSafety Commissioner, the Parliament, the age assurance industry and others.

The Roadmap for Age Verification

In 2019, the House of Representatives Standing Committee on Social Policy and Legal Affairs commenced an 'Inquiry into age verification for online wagering and online pornography'. The Committee published its final report entitled 'Protecting the Age of Innocence' in February 2020. The Committee recommended that the Australian Government direct and resource the eSafety Commissioner to develop a roadmap for the mandatory age verification for online pornography. That recommendation was supported by the Australian Government.

In March 2023, the eSafety Commissioner published a document entitled 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography' (**'Age Verification Roadmap'**). A background report including evidence and analysis supporting the Roadmap was also published.

The Roadmap was self-described as a 'high level summary of safety analysis and findings'. It set out next steps for safety recommendations to the Australian Government and suggested relevant factors to consider as part of the forthcoming Independent Review of the Online Safety Act 2021.

The eSafety Commissioner observed that age assurance on its own would not address the issue of online pornography and children. To the extent that it could serve to increase the age at which children encounter online pornography, making it more likely that they are equipped with the critical reasoning skills and context to interpret what they are seeing, age assurance could serve as a key component of an holistic response to preventing and mitigating that harm. Other countries are at different stages of considering and implementing measures. The online

industry itself is increasingly adopting more robust approaches beyond asking users to self-declare their age. Nevertheless, significant gaps remain.

According to the research undertaken by eSafety, more than three in four Australian adults support government implementation of age assurance for online pornography. There are, however, concerns about effectiveness, privacy and security. Those themes and concerns about accessibility, fairness and bias were echoed by young people and multi-sector stakeholders.

Key findings supporting the Roadmap, in brief summary, were as follows:

(1) Expectations and requirements for service providers within the online industry to apply age assurance and other complementary measures to prevent, or limit, children's access to online pornography should be established. An Independent Review of the Act required by January 2025, would provide an important opportunity to consider potential issues for reform identified in the process of developing the Roadmap. Lessons could be learned from the challenges which other regulators have encountered in enforcing age assurance requirements in other jurisdictions.

(2) The legislative and regulatory framework should establish a regulatory scheme for the accreditation and oversight of age assurance providers. The purposes of such accreditation were said to be to promote privacy, security, strong governance, transparency, trustworthiness, fairness and respect for human rights. The eSafety Commissioner observed that based on their consultations, there was unlikely to be any existing regulator or accreditation body that had the full breadth of experience and the capacity to provide all the necessary functions.

The Roadmap made reference to complementary measures for an holistic approach. Efforts by providers to ascertain their users' ages would only be beneficial if supported by complementary measures to create a safe and age-appropriate experience.

There was said to be a risk that measures would deter users from accessing compliant sites. Instead they might move to sites which did not comply with age requirements. For that reason consideration should be given to complementary interventions in other parts of the digital ecosystem to prevent children from landing at high risk sites and services in the first place.

Reference was made to other countries, including France, Germany and the UK considering or implementing age assurance requirements. Examples of age assurance measures were cited:

(1) Roblox: A game creation platform. In announcing a new Chat with Voice feature in September 2021, which would allow players to communicate with one another, Roblox said this would be available for early access to all users who verify they are at least 13 years of age though an ID scan accompanied by a selfie match to ensure 'liveness' and 'likeness'.

(2) Google in March 2022 announced a new age verification step for Australian users of YouTube. When attempting to access age restricted content on YouTube or downloading on Google Play, some Australian users may be asked to provide additional proof of age. Google would use that additional step to assure whether a user was above 18. If Google were unable to substantiate that the user was over 18, the user would be asked to verify age by providing a photograph of a government-issued ID or by allowing an authorisation on a credit card.

(3) Yubo, a location based social media app for teenagers introduced an age verification system in partnership with Yoti in May 2022. This was to allow users to be confident they are interacting with others of a similar age group. Yubo launched Yoti's facial age estimation technology for users aged 13 to 14 initially with a view to scaling the technology across its entire user base.

An independent assessment of age assurance mechanisms commissioned by eSafety found that facial analysis tools which use machine learning models to estimate a person's age based on their facial proportions and characteristics (and which then delete the image) were the most viable and privacy-preserving within the biometrics category. It was acknowledged that there were concerns that such technologies can create barriers to inclusion as they may not perform well for some skin tones, genders or those with physical differences.

Voice-age analysis and capacity assessment tools were said to be less mature. Testing of voice analysis and capacity testing tends to be limited by the fact that a person's ability to read, speak or write does not always correlate to their biological age. Accents, low language fluency or disability can also potentially create barriers to inclusion.

The use of hard identifiers to verify a person's identity including their age was tested. The identifying information is stored on the user's mobile device and is capable of being reused when needed. This can, of course, create barriers for those who do not have access to such documents.

The main finding from the independent assessment was that the age assurance industry and its associated technologies are new and still evolving. It was suggested that age assurance technologies be trialled in the Australian context before being prescribed. Enex Testlab supported the development of an internationally defined age token and the provision of multiple accredited options for consumers to select their preference for proofing their age. There were benefits in storing tokens at the device level through digital wallets.

In Recommendations for the Australian Government, the eSafety Commissioner proposed:

(1) The funding of specialist researchers and experts in working with younger children on sensitive issues to conduct research examining a number of matters relevant to encounters with online pornography.

(2) That the Government develop, implement and evaluate a pilot before seeking to prescribe and mandate age assurance technologies for access to online pornography.

This recommendation proposed a trial of age assurance technologies and the use of digital tokens in the Australian context.

It was proposed that a regulatory scheme be established for the accreditation and oversight of age assurance providers. There is already substantial work underway to develop a framework for Australia's digital identity system. This should be built on to establish a similar regulatory accreditation regime to the Trusted Digital Identity Framework for age assurance. Importantly, the eSafety Commissioner observed:

> Based on our consultations across government, at this stage, there is likely no existing regulator or accreditation body that has the full breadth of experience and capability to provide all the necessary functions, particularly in relation to this type of digital accreditation. However, building on the work of equivalent accreditation regimes in government such as the Trusted Digital Identity Framework could provide a good basis for starting discovery work on how an accreditation scheme could operate.[109]

[109] eSafety Commissioner, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography, March 2023, 35.

Next proposed steps by eSafety included the production of guidance to support providers in determining reasonable steps to implement expectations relating to measures to prevent children's access to online pornography, including age assurance and complementary measures.[110]

It is notable that eSafety's research found that 47% of 16 to 18 year old participants who had seen online pornography, first encountered it when they were 13, 14, or 15 years old. This was broadly consistent with other Australian research which found that the average age of children first viewing online pornography was 13.[111]

The Commonwealth Government's response to the Roadmap

The Government published a 'Response to the Roadmap for Age Verification' on 31 August 2023. In relation to age verification the Response included the following:

> 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.

110 eSafety Commissioner, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography, March 2023, 38.

111 Ibid 47 citing J Power, S Kauer, C Fisher, R Chapman-Bellamy & A Bourne, The 7th National Survey of Australian Secondary Students and Sexual Health, (ARCSHS Monograph Series No. 133). Melbourne: The Australian Research Centre in Sex, Health and Society, La Trobe University, 2022, DoI: 10.26181/21761522.

> 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.[112]

eSafety Commissioner's Statement following Government response to the Roadmap

In a statement published by the eSafety Commissioner and following the Government response, a number of 'next steps' were set out, including:

- Supporting industry associations to draft a set of industry codes to limit children's access to 'class 2' material, which includes online pornography.
- Contributing to the review of the *Online Safety Act*, advising on the suitability of existing regulatory powers to address children's access to online pornography.
- Raising awareness and providing practical guidance for appropriate interventions across the digital ecosystem through Safety by Design Initiative and 'Tech trends and challenges' program as well as broader industry engagement.

The Age Verification Providers' Association

The Age Verification Providers' Association ('AVPA') provided input to this Examination through Mr Iain Corby, its Executive Director. The AVPA was established in 2018. It is a not-for-profit global trade body representing 30 providers of what is said to be 'privacy-preserving online age assurance technology'. The information provided by the AVPA identified the species of the age assurance genus, being age verification and age estimation. Existing methods of age verification were identified as follows:

- Government issued physical ID — passports, driving licences, military/veteran ID
- Digital ID — government issued or privately provided reusable digital ID
- Bank Records — age can be confirmed by the user logging into online banking and agreeing to share it with a third party

---

[112] Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Government response to the Roadmap for Age Verification, August 2023, 2–3.

- Mobile Data Network Providers — in the UK, all new mobile devices are issued with a block on adult content that is only removed once the user proves they are 18 years or older

- Authoritative Database**s** — user supplied details such as name, address and date of birth confirmed with a credit agency

The existing methods of age estimation include:

- Facial age estimation

- Email address analysis

AVPA contended that both age verification and age estimation could be applied to South Australia to support the introduction of a legal minimum age for accessing social media.

In a letter Mr Corby discussed age assurance mechanisms in further detail.

Age estimation involves validation of a user's specific date of birth which may be derived from physical identity documents such as passports, their reusable digital equivalents or from accessing online banking or making one-way blind checks of authoritative databases.

Age estimation uses artificial intelligence to calculate the likely age range of a user based on biometric features or behaviours. The best known example cited had been independently tested by the US Government to deliver results with a mean average error of as little as 3.1 years. Voice print analysis is also in use. Another approach relies on hand movements which can be shared using a camera phone or webcam accessed by artificial intelligence. This is said to be very new and currently under independent verification by the industry. Although estimation was said not to yield an exact result, it could create an effective safety net to prevent children significantly younger than the minimum age from gaining access. So South Australia, it was suggested, could 'pragmatically' require that users appear to be at least 13 to an estimation tool which has been tested to meet a maximum mean average error of one and a half years and simply accept that while some 11 and 12 year olds might pass the test, very few younger children would be able to do so. This, it was said, would be a major step forward from a situation whereby a 5, 7 or 9 year old can access social media without any checks.

There has been some concern expressed by the UK Regulator OFCOM about false negatives — where someone who is old enough to access social media is refused an account as a result of being estimated to be younger than the minimum age. One approach would be to set the age tested by estimation above the legal minimum. A test that users appeared to be at least 15 would remove most false positives from that process (namely users who are actually under 13 but who pass the estimation test even when set two years old). It would then require more users who fall into the false negative category to find an alternative way to verify their age.

Other jurisdictions that have implemented limitations on social media access for children were mentioned and in that context recent publications by OFCOM in the UK addressing the topic of age assurance in great detail.

Mr Corby also provided a consultation document prepared for the purposes of what is called the 'euCONSENT' project, which is the specification for a new industry-wide ecosystem to allow for interoperable use of age checks so that a single check could be used across multiple platforms. The document set out technical specifications and was dated August 2024. The ecosystem it described was designated as 'AgeAware'.

The system proposed would leave the primary duty to provide an age appropriate online experience with the digital service provider. By using tokens which could be stored on a device for a predetermined period of time the AgeAware approach was also said to achieve many of the benefits of the alternative device approach being promoted by some age restricted digital service providers. It did not transfer the costs and liability of performing age assurance from those providers to the owners of the operating systems or app stores who had been clear that they did not wish to assume that responsibility,

The way in which AgeAware would operate with respect to a particular user for the first use was said to be as follows:

a. User attempts to access an age-restricted website or application, collectively termed 'digital service providers' (DSP).

b. User is directed by the digital service to the AgeAware App (essentially a mini-website hosted on the User's own device).

c. User selects an Age Assurance Provider (AAP) and undergoes an age assurance check (which can be either age verification or age estimation, subject to the level of assurance required).

d. Upon a successful check, with their consent, a token is placed on the user's device.

e. User agrees to submit the token to one or more DSPs.

f. The DSP receives the token (with no personal data beyond the answer to the age-related qualification question thanks to the function of the Anonymisation Service).

g. The user is directed back to the Digital Service to access if qualified.

h. The tally service records this use of an AAP's token with a DSP to enable billing.[113]

Google, TikTok, Meta and Snap

Meetings were held with representatives of Google, TikTok, Meta and Snap. An account of their practices and policies is set out in a separate chapter. However, specific reference to their age assurance measures is suitable for inclusion in this chapter.

Google Australia has been operating in Australia for 23 years. Its parent company, Google LLC, is an American multi-national corporation. Thirteen years is the minimum age requirement to manage a personal Google account, save for select countries in Asia, the Caribbean, Europe and South America where minimum age requirements range from 14 to 16. Parents of children under 13 can help create and manage a Google account with Family Link. Some Google services have specific age requirements. YouTube, Addsense and Google Ads all require users to be 18 or older. If Google learn that a user is not old enough to hold their own account, the user has 14 days to update the account to meet the age requirement or it will be disabled.

In TikTok's submission to the Joint Select Committee on Social Media and Australian Society in July 2024, it addressed age assurance. It maintains a neutral industry standard age-gate that requires individuals to provide their birth date to demonstrate they are at least 13 years old. The age-gate is said to be neutral in that it helps to discourage people from simply picking a pre-populated minimum age. They are not nudged towards the 'right' age.

In addition to the industry standard age-gate, TikTok uses technology and human moderation to help determine whether a user may be under age. Its Safety Moderation Team is trained to be alert to signs that an account may be being used by a child under the age of 13. It also uses

[113] Iain Corby, Alastair Graham, Ben Gower, 'AgeAware Specification: Consultation Document WP1:Business Requirements' (5 August 2024) 6–7.

other information provided by its users such as in-app reports from its community to help surface potential under age accounts.

If a user is suspected of being under the age of 13 years, the account is subject to human moderation. If a moderator concludes that an account belongs to an under age user it is removed. In 2023, TikTok removed more than 76 million accounts globally belonging to suspected under age users.

Meta representatives made the uncontroversial point that there is no guaranteed way at present to do age assurance online. To the extent that Meta carries out age assurance, it requires either the collection of personally identifying information, such as a passport or birth certificate, or the use of biometric data. There is a tension with privacy laws and Meta said it has done a lot of things to limit the use of children's data, particularly for advertising and for broader safety concerns over the years.

Meta referred to work that it had been doing with a third party provider called 'Yoti' based in Germany. Its technology, using face-based prediction, was said to be innovative and very interesting but highlighted the nascent nature of the technology and its uses. AI models had been in place with Facebook and Instagram for about 3 or 4 years which looked at the account holder's behaviour. For that mechanism to be effective, however, the user needed to be on the service and to have interacted or engaged with accounts and content over that time. There were options that could be applied where a user was checked or reported as a possible under age user, e.g. changing their age or trying to access content or engage in inappropriate behaviour. It was accepted that there are gaps in the industry's ability to enforce age limitations. There was said to be an industry-wide conversation about whether something could be done at the App store level in relation to age assurance — where credit card details have to be entered to download an app. That would usually mean some form of parental involvement.

Snap Inc, the provider of Snapchat, primarily a messaging service, also gave input to the Examination. All Snapchat users are required to be at least 13 years old. In its submission to the Joint Select Committee on Social Media and Australian Society, Snapchat stated that:

> We continue to explore options for age verification, and have been engaging closely with authorities around the world, including the eSafety Commissioner, for many years. Providing effective age verification or assurance that balances user safety, data

> privacy and security, fairness, accessibility and equity, is a persistent policy challenge with no clear solution.[114]

The Snapchat submission referred to the eSafety Commissioner's Roadmap and the Government's Response and identified two primary options for age assurance:

- ID-based solutions asking users to provide ID to verify their age; and
- age-estimation technology often involving the use of biometric data, such as a facial scan, to infer a person's age or age range.

Snap Inc agreed with the Government Response to the Roadmap that 'each type of age verification or age assurance technology comes with its privacy, security, effectiveness and implementation issues.' Snapchat also quoted the observation from the Government Response that the age assurance market is, at this time, immature.

Snap Inc said it continued to research age assurance mechanisms. Their view is that device level age verification is the best available option. Age collection is already part of the device ID process when registering a new device such as an iPhone or Android phone. The submission stated:

> Adding a level of age verification to this step, and then making this verified age available to all services, would simplify the process for users, reduce the risk of repeatedly providing sensitive ID data to a wide range of apps, and avoid consent fatigue. Users would only need to confirm their age once, which also increases the odds that the information will be accurate. If age is collected and checked at the device level, then that information could be used within the app store to show apps appropriate for the user's age (meaning that age-inappropriate apps couldn't be accessed or downloaded; users under 13 would be prevented from viewing or downloading apps that are designated 13+).[115]

It was also suggested that during the app signup process, apps could receive age signals directly from the device. They could also communicate back to the device operators if there appeared to be any reason to doubt the assured age signals. If an online communication platform became aware that a user was under the assured age, they could notify the device operator so that the account user's age could be checked again.

---

114 Snap Inc, Submission No 40 to the Joint Select Committee on Social Media and Australian Society (26 June 2024) 7.

115 Ibid 8.

Snap Inc stated its belief that leveraging the potential of device-level age verification could drive significant progress in what has remained an intractable policy challenge until now.

Age assurance trial — May 2024

In May 2024, the Australian Government announced an 'Age Assurance Trial' encompassing both age verification and age estimation technologies, to explore their efficacy in protecting children from encountering pornography and other high-impact online content.

As is apparent, the results of such a pilot will be relevant to assessment of age assurance technologies available to support any South Australian legislation. What is available from time to time will, no doubt, inform the reasonable steps necessary for social media service providers to comply with a duty not to allow access to their services by children within the restricted age range up to the age of 14, or to require parental consent for children aged 14 and 15.

eSafety's Tech Trends Issues Paper on Age Assurance — July 2024

In July 2024, the eSafety Commissioner published a Tech Trends Issues Paper on Age Assurance and its role in online safety. The paper captured developments following the publication of the Roadmap and considered age assurance for a range of uses. The following table from the paper sets out examples of the current use of age assurance measures in Australia by different platforms.[116]

Platform	Age Assurance Measures
YouTube (Google)	• Users in Australia can confirm their age by providing credit card details or a valid government ID (age verification). • Uses machine learning to identify potential underage users (age estimation) and requires those users to provide verification of their age (using credit card details or a valid government ID).[117] • Classifiers identify 'young minors' livestreaming who are assessed by a human moderator.
Yubo	• Verifies the age of all users using facial age estimation or user ID.[118]

116 eSafety Commissioner, Tech Trends Issues Paper: Age Assurance, July 2024, 7-8.

117 See further "Google Account Help- Update your account to meet age requirements", https://support.google.com/accounts/answer/1333913?sjid=4585256672698072826-AP#zippy=%2Cuse-a-credit-card%2Ccheck-the-status-of-your-request%2Cuse-a-government-id.

118 See further, "Yubo New Age Verification Feature Helps Keep You Safe", https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe

Instagram (Meta)	• Users must provide a date of birth when creating an account. • If a user in Australia later attempts to amend their age to be over the age of 18, they must confirm their age by submitting a government ID or by taking a video selfie using facial age estimation technology.[119]
TikTok	• Users must provide a date of birth when creating an account. • Uses automated and human moderation to detect underage users. • If a users' account is mistakenly shut down, they can demonstrate they are over 13 using facial age estimation technology, credit card or a selfie with government ID.[120]
Tinder	• Verification is not required to create an account. • Is trialling ID and photo verification to protect users from scams.[121]
Roblox	• Uses Persona (an online verification company) to verify users' age using a government ID and real time matching to photo identification.[122] • Age verified users over the age of 17 are given access to suitable content and experiences.
Snap	• Users must provide a date of birth when creating an account. • If made aware a user is under the age of 13, the account is terminated and the user's data deleted. • Prevents users between the age of 13 from updating their year of birth.[123]
Twitch	• Uses measures including, self-declaration on sign up, analysis of text entered and traffic and parental report submissions.[124]
Alcohol (NSW)	• Piloting the use of the Service NSW app as proof of age for online alcohol purchases.[125]

119 See further, "Introducing New Ways to Verify Age on Instagram", https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.

120 See further, "Underage appeals on TikTok", https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok.

121 See further, "Tinder announces ID Verification pilot in Australia and New Zealand", https://au.tinderpressroom.com/news?item=122572.

122 See further, "Age ID Verification", https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification.

123 See further, "About underage bans on TikTok", https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#1.

124 See further, "Guide for Parents and Educators", https://safety.twitch.tv/s/article/Guide-Parents-Educators?language=en_US.

125 See further, "Same day delivery age verification requirements", https://www.liquorandgaming.nsw.gov.au/resources/same-day-delivery-age-verification-requirements.

Online gambling platforms	• Are required to verify users are over 18 before they place a bet. • Sportsbet allows users to verify their age using driver's licence, passport, Medicare card, or superannuation or payroll information.

How and When Age Assurance Technologies Can be Implemented [126]

In summary, according to the Tech Trends Issues Paper, age assurance measures can be implemented at various junctures of a user's interaction with a platform, including:

- **Accessing a specific site, app or service** requiring all users to declare or verify their age before they can access the site/platform.
- **Proactive detection** using technology or human moderators to remove underage users.
- **Account sign up** requiring users to declare their age/date of birth at the point of sign up.
- **Accessing specific features or content on a service** requiring users to verify their age to access features or content not suitable for children.
- **Adjusting a previously entered age,** users attempting to change their age to access a site, app, service or specific features/content.
- **Responding to a flag or report** indicating a user's actions suggest they are not their declared age, via a report from other users or AI behavioural scanning.[127]

eSafety supports measures that involve all stages of the ecosystem of online services, including operating systems, app stores, and search engines.[128]

Examples of key points at which age assurance can be implemented in the provision of online services or products were:

- Connecting to the internet — in the United Kingdom mobile network operators block 18+ content on their services unless a user proves that they are an adult. This can be

126 Tech Trends Issue Paper, above n 116, 9-10.
127 Ibid, 9.
128 Ibid, 10.

done online or over the phone with a credit card or installed with a photo ID. The Tech Issues Paper commented that OFCOM's draft guide in supporting the implementation of the UK *Online Safety Act* suggested that this check could be shared with other services as a valid age check. In Australia ISPs keep details of the accountholder who is typically over 18. They offer parental controls and filtering options, but those are not default settings and are not linked to age checks.

- Device level — native apps on device operating systems such as Apple's Screentime, Google's Family Link and Microsoft's Family Safety, were said to offer parental control and filtering options. That infrastructure could be used for age checks to ensure features, apps, sites and services used on devices are age appropriate.

The Tech Trends Issues Paper also observed that such age check points could rely on age attributes shared by the user across an ecosystem. Ecosystems of online services were said to exist where products, including online services, are interconnected, e.g. through integration, pre-installation and common user accounts. eSafety stated its support for a response that involved all services, products and platforms such as devices' operating systems, app stores and search engines, in reducing access to content that may not be age appropriate.

Privacy, security and data collection

The Tech Trends Issue Paper addressed privacy and security issues. Age assurance and age estimation technologies pose privacy risks due to the type and volume of data and biometric information they collect, store and use.[129] The eSafety Commissioner noted the following strategies which may reduce those privacy risks:

- **Implement enforceable standards** for oversight and independent verification of age verification systems and providers (including complaint and redress mechanisms).

- **Design systems and processes to minimise data use** by only collecting data for its intended purpose. Integrally '[w]hile IDs are often used to verify age**, it is not necessary to identify users to determine their age**. (emphasis in original)

129 Ibid 11.

- **On-device age analysis** by performing age verification on the user's native device and deleting the input once the analysis is complete.

- **Use re-usable verifications or 'tokens'** which can be limited to confirming whether a user meets the minimum age requirement to use a site/service.

- **Apply a double-blind or zero-knowledge proof method** to share an estimated/verified age to a verifying party without revealing further details.[130]

Comment — Age assurance mechanisms limited to State-based users

A particular issue arises in relation to the application of age assurance mechanisms in response to requirements of a State law with an age based restriction on access to social media that is not reflected in the Commonwealth law. In order to comply with a State-based prohibition or duty which is specific to the particular State, it will be necessary for the provider to know where the user lives before applying the State-specific age assurance mechanism. At the lowest level this may be done by requiring all users in Australia to provide the user's postcode. The question that then arises is what means may be applied to verify the correctness of the asserted postcode. Obviously, a young person within the restricted age range and aware of the geographical limitation of the restriction could provide a postcode for another State.

A further step might be to require the provision of a residential address which could be checked against Commonwealth electoral rolls. This geographical requirement highlights the limitations of any purely State-based restriction. That in turn highlights the desirability of a uniform national approach rather than a mosaic of State-based restrictions which would generate significant challenges in terms of compliance.

130 Ibid.

Chapter 9: Practices and policies of major social media service providers

A number of social media service providers gave input to the Examination about their practices and perspectives on online safety for children. It was made clear at each meeting with providers that it was not open to the Examiner to canvass the policy settings adopted by the South Australian Government. They defined the parameters within which the legal examination is being carried out. Nevertheless it was important that the Examination be informed by current online child safety practices adopted by social media service providers and their comments on the proposed model of a generic definition of 'social media service' attracting the access restriction, together with a carve-out for exempt social media services. These meetings also provided an opportunity for discussion of age assurance mechanisms already put in place by providers for particular classes of service or material.

What appears below is an outline of the materials submitted by major social media service providers.

Google

Ms Lucinda Longcroft, Director Government Affairs and Public Policy Australia and New Zealand at Google and Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy for YouTube met with the Examiner on 12 August 2024 and discussed the legislative model under consideration by the Examiner.

An outline of the nature and relevant practices and policies of Google Australia follows.

About Google Australia

Google has been operating in Australia for 23 years. Its parent company is Google LLC, an American multinational corporation and technology company focusing on online advertising, search engine technology, cloud computing, computer software, quantum computing, e-commerce, consumer electronic and artificial intelligence.

Google was originally written as a search engine, determining a website's relevance by the number of pages and analysing the relationship among websites.

In its current form, Google enables users to search for information on the Internet by entering keywords or phrases through the Google Search function. The main purpose of Google Search is to search for text in publicly accessible documents offered by web servers, as opposed to other data, such as images or data contained in databases. Google Search uses algorithms to analyse and rank websites based on their relevance to the search query.

Google is the most-visited website worldwide, followed by Facebook and X. Google is also the largest search engine, mapping and navigation application, email provider, office suite, online video platform, photo and cloud storage provider, mobile operating system, web browser, machine learning framework, and AI virtual assistant provider in the world as measured by market share.

Age restrictions

Thirteen years is the minimum age requirement to manage a personal Google Account, except in select countries in Asia, Caribbean, Europe, and South America where the minimum age requirements range from 14 to 16. Parents of children under 13 can help create and manage a Google Account with Family Link. Some Google services have specific age requirements – YouTube, AdSense (18+) and Google Ads (18+). If Google learn a user is not old enough to hold their own account, the user has 14 days to update the account to meet the age requirement or the account will be disabled (more information below).

Disabled Account

Once Google have ascertained a user is not old enough to have their own Google Account, the user has 14 days to either set up supervision for the account (with their parents) or verify they are old enough to manage the account. During this grace period, the user can log in and use the account as normal. If the user chooses neither of these options, after 14 days the account will be disabled, and account information deleted after 30 days. Once the account is disabled, all published content is hidden.

How does Google manage harmful content?

Google uses AI based protections to restrict exposure to abusive content, for example:

- Gmail automatically blocks nearly 10 million spam emails from inboxes every minute and Search has tools to prevent Autocomplete from suggesting potentially harmful queries.
- Automatic detection helps YouTube remove harmful content efficiently, effectively and at scale – in Q2 of 2023, 93% of policy-violative videos removed from YouTube were first detected automatically.
- Google also implements 'safety guardrails' in their generative AI tools to minimise the risk of their being used to create harmful content.

In addition, according to Google, each of their products is governed by a set of policies that outlines acceptable and unacceptable content and behaviours.

Content safety

Preventing abuse

Google uses AI-backed protections to keep people safe from abusive content. Gmail automatically blocks nearly 10 million spam emails from inboxes every minute and the Search function has tools to prevent the AutoComplete feature from suggesting potentially harmful queries. Each of Google's products is governed by a set of policies that outlines acceptable and unacceptable contents and behaviours.

Detecting harmful content

AI helps Google scale abuse detection across their platforms. AI-powered classifiers help quickly flag potentially harmful content for removal or escalation to a human reviewer. Google also works with outside organisations who flag content they think might be harmful. Both Google and YouTube take feedback from hundreds of Priority Flaggers, organisations around the world with cultural and subject-matter expertise who escalate content for review.

Responding appropriately

Google relies on both people and AI-driven technology to evaluate potential policy violations and respond appropriately when content is flagged. When the content violates their policies, they can restrict, remove, demonetise or take account-level actions to reduce future abuse. A creator or publisher can appeal decisions.

Parental controls

Family Link

The Family Link app can be used to create a Google Account for a child under 13, and to add supervision to a child's existing Google Account. The Family Link app allows a parent to:

- Change some of the child's Google Account settings.
- Manage the child's apps on supervised devices: Decide which apps the child can download or purchase, block or allow the, and change app permissions.
- Manage the child's screen time on supervised devices: Set a bedtime or daily screen limits and see how much time your child spends on certain apps.
- Check the location of the child's Android or compatible Fitbit device.
- Restrict mature content on Google Play.

How Google is used in educational settings

Google Classroom

Google Classroom is a free blended learning platform developed by Google for educational institutions that aims to simplify creating, distributing, and grading assignments. The primary purpose of Google Classroom is to streamline the process of sharing files between teachers and students. As of 2021, approximately 150 million users use Google Classroom.

Google Classroom uses a variety of proprietary user applications (Google Applications for Education, more information below) with the goal of managing student and teacher communication. Students can be invited to join a class through a private code or be imported automatically from a school domain. Each class creates a separate folder in the respective user's Google Drive, where the student can submit work to be graded by a teacher. Teachers can monitor each student's progress by reviewing the revision history of a document, and, after being graded, teachers can return work along with comments and grades.

Google Applications for Education

Google Applications for Education is a service from Google that provides independently customizable versions of several Google products using a domain name provided by the customer. It features several Web applications with similar functionality to traditional office suites including emails, calendar, file storage, word processing, spreadsheets, presentation, instant messaging, and discussion groups.

Google Meet

In 2020, Google added integration with Google Meet so teachers can have a unique Meet link within each class. Google Meet is a video communication service and was formally launched in March 2017. The service was unveiled as a video conferencing app for up to 30 participants, described as an enterprise-friendly version of Hangouts. Google Meet has 1:1 and group video calling capability. When a user uses Meet, some data is processed to offer better experiences with the product, and the information stays secure. Privacy settings are controlled in the users Google Account. The audio and video are encrypted end-to-end and not stored on Google servers. Messages sent in the Meet app are stored encrypted on the servers. If live captions are turned on, Google uses audio data which is not linked to identifiable information and not stored. If a meeting is recorded, the data is stored in Google's data centres, and encrypted in transit and at rest.

What is YouTube?

YouTube is an online video sharing and social media platform operated by Google LLC (1600 Amphitheatre Pkwy, Mountain View, CA 94043, United States).

Launched in 2005, YouTube is now the second most visited website in the world after Google Search. As of January 2024, YouTube has over 2.7 billion monthly active users.

YouTube allows users to interact, share content, and create a community around videos. People can like, comment, and subscribe to channels, within a social environment where creators and viewers can engage with each other. This interactive aspect is a hallmark of social media platforms.

Users can upload, share, and view videos, and the platform supports various features like YouTube Kids, YouTube Music, YouTube Premium, and YouTube Shorts.

YouTube generates revenue primarily through advertisements and offers a paid subscription option for ad-free viewing. It is a platform where individuals and corporations can create and expand their reach by sharing and monetizing their content.

YouTube Kids

YouTube Kids is a child-friendly app offering a curated selection of content from YouTube. It is governed by policies to ensure videos are suitable for children, and features parental controls, including the ability to turn search on or off. The app's search ranking considers content quality and safety, with automated filters and human oversight ensuring age-appropriateness. Search results are also personalised based on a child's watch history and parental content settings. Despite these measures, there is a small chance of encountering unsuitable content, which can be reported to further refine the app's offerings.

> Note: YouTube handles tremendous breadth, depth and scale of content. So while we work hard to get it right, there's always a chance that your child will find content that you don't want them to watch. If this happens, you can report the video. We use this information to improve YouTube Kids for everyone.[131]

YouTube Kids profiles

YouTube Kids allows signed in parents to create a separate profile for each kid in their household. Each profile has a separate set of viewing preferences and recommendations, allowing multiple kids to get the most out of the YouTube Kids app.

Profiles are available on devices where:

- The parent is signed in; and
- YouTube Kids app is installed.

You can have up to eight profiles.

Note: You can also use YouTube Kids without signing in at all.

---

131 YouTube 2024, 'YouTube Kids', available at: https://www.youtube.com/intl/ALL_au/howyoutubeworks/product-features/search/#youtube-kids

How videos available in YouTube Kids are selected

One option is to allow a child to explore all videos on YouTube Kids. Parents can choose between three age-based content settings:

- Preschool (Ages 4 & under)
- Younger (Ages 5—8)
- Older (Ages 9—12)

YouTube's automated systems select content from the broader universe of videos on YouTube, excluding content not suitable for kids. If a user finds something inappropriate, the user can block it or report it for review.

Another option is for a parent or caregiver to handpick the content a child has access to. The child cannot use the search function under this option. For more info on this option, please refer to the YouTube Kids guide to parental controls and settings, available at: https://support.google.com/families/answer/10495678?hl=en.

Note: If a child is over 13 years old (or the applicable age in their country or region) and chooses to manage their own account, a parent or caregiver will not be able to supervise their experience on YouTube with the controls above.

How a child can discover videos in YouTube Kids

- Using the search function (YouTube Search),
- Videos on the home screen,
- Recommended videos, or
- 'Watch it again'.

Further information on these elements is provided below.

What parental controls are available in YouTube Kids?

- Setting a timer to limit how much time a child spend on the app,

- Blocking content,
- Limiting access to only approved content,
- Turning off the search function,
- Clearing history, and
- Pausing history.

Search function – YouTube Search

YouTube's search system ranks videos by relevance, engagement, and quality to deliver the most useful results for the user's query. Relevance is judged by how closely a video's details match a user's search terms. Engagement is gauged by user interactions, like watch time, to assess a video's relevance. Quality is determined by the channel's credibility on the topic. Additionally, the personalised search history of the user is used to tailor results, making them unique to each user.

Recommended videos

Recommendations drive a significant amount of the overall viewership on YouTube, even more than channel subscriptions or search. YouTube's recommendation system enables users to find recommendations in two main places: their homepage and the "Up Next" panel. The homepage is what a user sees when they first open YouTube—it displays a mixture of personalised recommendations, subscriptions, and the latest news and information. The Up Next panel appears when a user is watching a video and suggests additional content based on what they're currently watching, alongside other videos that YouTube think they may be interested in.

Recommendations on Up Next

YouTube's recommendation system compares viewing habits with those that are similar to a user and uses that information to suggest other content an individual may want to watch. So if a person likes tennis videos and our system notices that others who like the same tennis videos also enjoy jazz videos, and the user may be recommended jazz videos, even if they have never watched a single one before (for categories like news and information, this might function differently).

News and information

For content where accuracy and authoritativeness are key, including news, politics, medical and scientific information, we use machine-learning systems that prioritise information from authoritative sources and provide context to help you make informed decisions.

YouTube Live

Creators can live stream on YouTube via webcam, mobile or encoder streaming. Webcam and mobile are considered great options for beginners and allow creators to go live quickly. Encoder streaming is applicable to more advanced live streams such as: sharing the creator's screen or broadcasting gameplay, connecting to external audio and video hardware and managing an advanced live stream production (like multiple cameras and microphones).

Live chat moderation tools

YouTube offers live chat moderation tools to help prevent harassment. Some of these tools include assigning moderators, a blocked words list, holding inappropriate chats for review, slow mode and turning off live chat.

YouTube management of harmful content

YouTube's Community Guidelines are a set of rules that outline what type of content is and is not allowed on the platform. These guidelines apply to all types of content on YouTube, including videos, comments, links, thumbnails, and more. A summary of the key areas covered by the guidelines is provided below:

- Spam and Deceptive Practices: Content intended to scam, mislead, spam, or defraud users is not allowed. This includes fake engagement and impersonation.
- Sensitive Content: Rules are in place to protect viewers, especially minors, from harmful content. This includes policies on nudity, sexual content, child safety, and self-harm.
- Violent or Dangerous Content: Content that promotes hate speech, predatory behaviour, graphic violence, malicious attacks, or harmful behaviour is prohibited.

- Regulated Goods: The sale of illegal or regulated goods or services, including firearms, is not permitted on YouTube.
- Misinformation: Misleading or deceptive content that poses a serious risk of egregious harm, such as promoting harmful remedies or interfering with democratic processes, is banned.

YouTube also allows for an Educational, Documentary, Scientific, and Artistic (EDSA) exception, where content that might otherwise violate the guidelines can stay on the platform if it has significant educational, documentary, scientific, or artistic value.

Creators who wish to monetise their content must also comply with YouTube's Monetisation Policies in addition to the Community Guidelines.

A YouTube channel is terminated if it accrues three Community Guidelines strikes in 90 days, has a single case of severe abuse (such as predatory behaviour), or is determined to be wholly dedicated to violating its guidelines (as is often the case with spam accounts). When a channel is terminated, all of its videos are removed.

YouTube's most recent Community Guidelines Enforcement Report is available at: https://transparencyreport.google.com/youtube-policy/removals?hl=en&total_removed_videos=period:2024Q1;exclude_automated:all&lu=videos_by_country&videos_by_country=period:2024Q1;region:;p:1.

Google — Public commentary

Google and YouTube made a submission to the Joint Select Committee on Social Media and Australian Society. Some key points from their submission are listed below.

Age-appropriate online experiences on YouTube

- Google does not allow children under 13 years to create a standard Google/YouTube account. For individuals under this age bracket, Google offers a dedicated service, YouTube Kids, to provide content for children. This platform has strict parental controls and a far more limited corpus of content.
- Google employs systems to protect young people from harmful content on YouTube, including:

- Preventing age-sensitive add categories and prohibiting ad-personalisation for users under 18.

- YouTube's community guidelines prohibit harmful content including pornography and sexually explicit content, content that is harmful or exploitative to children, content that encourages dangerous or illegal activities or suicide or self-harm, from appearing on the platform at all.

- For content that does not breach these guidelines but is flagged as 'mature', YouTube restricts accounts belonging to users under 18 from viewing the content.

Google's proposed legislative framework

Google suggested the following principles be included in a legislative framework aimed at keeping children safe online:

- Require online services to prioritise the best interests of children and teens in the design of their products.

- Take a risk-based approach when requiring age assurance.

- Increase protections for teens between the age of parental consent and 18, in a manner that respects their increased maturity.

- Address the need for robust parental control options that also respect the increased abilities and autonomy of teens.

- Require online services to take measures to support mental health and wellbeing for children and teens.

- Ban personalised advertising for children and teens.

- Require platforms to give teens and parents of children tools to manage the use of their online viewing and search history in personalised recommendations.

- Require platforms to take a responsible and transparent approach to developing and enforcing content policies.

    - Use risk-based impact assessments to foster accountability.

- Encourage regulatory harmonisation and global interoperability.
- Recognise differences among services.

Snap Inc

Mr Henry Turnbull, Head of Public Policy, Asia Pacific and Mr Ben Au, Manager, Public Policy, Australia and New Zealand for Snap Inc met online with the Examiner.

An outline of the background and the practices and policies of Snap Inc, prepared from materials provided to the Examination is as follows:

Snap Inc is a technology company founded in 2011 and is based in Santa Monica, California. The company develops technological products and services, namely Snapchat, Spectacles, and Bitmoji. The company was named Snapchat Inc. at its inception, but it was rebranded Snap Inc. on 24 September 2016, in order to include the Spectacles product under the company name.

Snapchat

Snapchat is a communications service designed for people ages 13 and up, and one of its principal features is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients. It is very popular with teenagers and young adults, who primarily use it to talk with their close friends, similar to the ways they interact in real life. It is similar to how older generations use text or picture messaging to stay in touch with friends and family.

Parental Controls

Snapchat's Family Centre

Snapchat's Family Centre provides information on the controls available to parents, giving them oversight of who their children and teens are communicating with on Snapchat. Parents can view their child or teens' privacy and safety settings, manage parental controls, and report any concerns directly to the Snapchat Trust and Safety team.

To access the Family Centre, parents need to:

- Download Snapchat to their device from their app store and create an account

- Ask their child or teen for the username and add them as a friend
- Once accepted as a friend, the Family Centre functionality can be used
    - Invite their teen to join. The teen will receive an information card and they must opt in to participate. A notification will be sent to the parent to say the teen has accepted the invitation
- The parent is now able to use the Family Centre to see who their teens are talking to and set content controls.

Privacy, Safety, Policy and Transparency

Community Guidelines

Snap has a clear set of Community Guidelines to help Snapchatters use the services safely. These rules prohibit illegal and potentially harmful content and behaviour such as sexual exploitation, pornography, selling illicit drugs, violence, self-harm, and misinformation. Snap applies additional moderation to the public content platforms, Stories and Spotlight, to prevent content that violates the rules from reaching a large audience.

To enforce against violations of the Community Guidelines and avoid any potential dangers, Snap uses both proactive detection tools and reports from Snapchatters, parents, and law enforcement. They have a 24/7 global Trust & Safety team that investigates these reports, and, in most cases, they take action within an hour in order to enforce Snapchat's safety standards. That can include warning users, removing content, banning an account, and escalating a report to law enforcement.

Privacy Principles

Snapchat makes a user privacy a priority by not stockpiling private messages and publicly showcasing a timeline of everything a user has ever posted. Snapchat is designed so a user's followers only see what the user elects to share. A user can decide if they want their 'Snaps' to be saved in Snapchat, and messages can be deleted at any time.

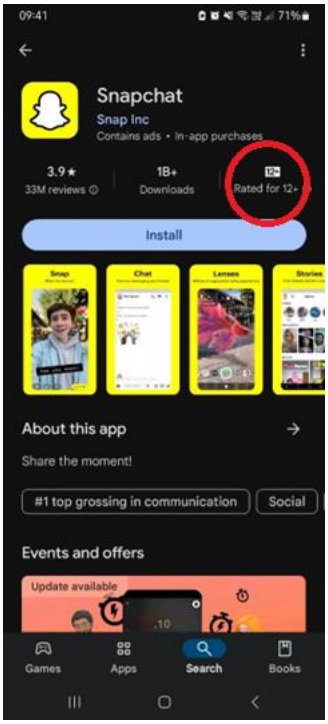
Safeguards for teens

Snapchat offers additional protections available through various control settings, and the principles and policy referred to above, including:

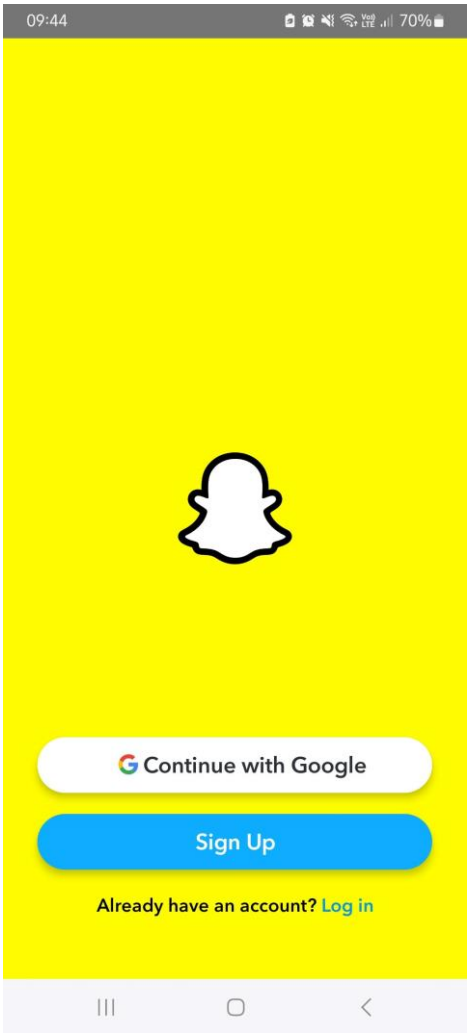
- Protections against unwanted contact
- Zero Tolerance for severe harms
- Age-appropriate content
- Strong default settings
- Quick and simple reporting tools
- Only for teens aged 13+

Signing up to Snapchat

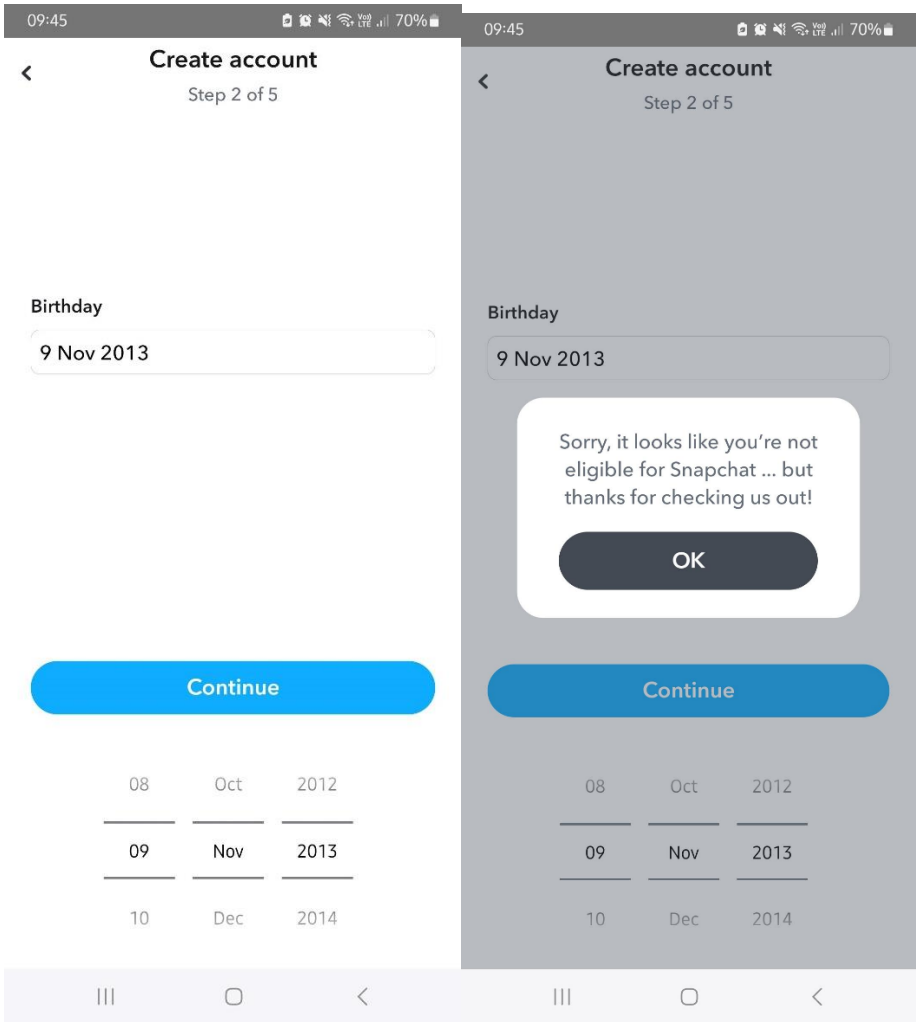
On Google Play, the age recommendation for Snapchat is 12+.



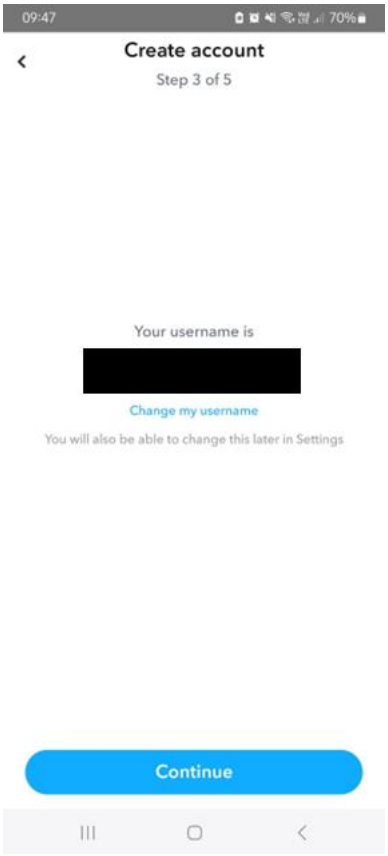
Users are able to sign in using an existing Google Account if they wish.



If a user put their actual birthdate in, Snapchat automatically refuses access. The user is then returned to the log-in screen.



Once inputting a birthdate making the user 13+, the user is advised their username, with no option to verify their age.



The user is then prompted to enter a password to complete the log-in.

Snap Inc — Public commentary

Snap Inc provided a submission to the Joint Select Committee into Social Media and Australian Society.

Snap Inc also attended a hearing at the Joint Select Committee on 28 June 2024 and answered various questions from the Committee Members.

In its submission to the Joint Select Committee, Snap Inc stated:

> We require all Snapchat users to be at least 13 years old, and if we identify that someone who's using Snapchat is younger than that, we will shut down their account. For those over the age of 13, we appreciate that the age at which young people start using Snapchat will often come down to a decision between parents and their teens. We recognise our role in supporting an informed conversation, and we provide parents with tools and resources, including through our online Parent's Guide and in-app Family Centre to help make appropriate choices for their teens.

On the question of age verification, the submission stated:

> We continue to explore options for age verification, and have been engaging closely with authorities around the world, including the eSafety Commissioner, for many years. Providing effective age verification or assurance that balances user safety, data privacy and security, fairness, accessibility and equity is a persistent policy challenge with no clear solution.

Snap referred to the eSafety Commissioner's Roadmap for Age Verification published in August 2023 and the Government's Response which it characterised as effectively highlighting the many challenges. It accepted, as outlined in the Roadmap, there are two primary options when it comes to age verification or assurance:

- **ID-based solutions:** asking users to provide ID to verify their age, and
- **Age-estimation technology**: often involving the use of biometric data, such as a facial scan, to infer a person's age or age range.

The submission stated:

> At Snap, we are continuing to research options and are hopeful that we can work together as an industry to develop an effective and practical approach. Our view is that **device level** age verification is the best available option. Age collection is already part of the device ID process when registering a new device, such as an iPhone or Android phone.
>
> Adding a level of age verification to this step, and then making this verified age available to all services, would simplify the process for users, reduce the risk of repeatedly providing sensitive ID data to a wide range of apps, and avoid consent fatigue. Users would only need to confirm their age once, which also increases the

> odds that the information will be accurate. If age is collected and checked at the device level, then that information could be used within the app store to show apps appropriate for the user's age (meaning that age-inappropriate apps couldn't be accessed or downloaded, users under 13 would be prevented from viewing or downloading apps hat are designated 13+).
>
> During the app sign-up process, apps could also receive age signals directly from the device. Moreover, apps could also communicate back to the device operators if they have identified any reason to doubt the assured age signals. If an online communication platform became aware that a user was under their assured age, they could notify the device operator so that the account user's age could be checked again.[132]

Snap Inc stated its belief that leveraging the potential of device level age verification could drive significant progress in a still intractable policy challenge. It asserted its commitment to 'working towards a solution that prioritises user safety, privacy and inclusivity.

Meta

A number of representatives of Meta provided input to the Examination at a meeting held on 19 August 2024. They were:

Mia Garlick, Regional Director, Policy for Japan, Korea, Aus, NZ and the Pacific

Mr Philip Chua, Director of Instagram Public Policy, APAC

Ms Malina Enlund, Safety Policy Manager, APAC

Ms Alex Cowen, Policy Programs Manager, Australia

Ms Bronwyn Lo, Public Policy Manager, Australia.

Background about Meta and relevant practices and policies were distilled by officers of the South Australian Government from material sourced from Meta's website and is reproduced below.

About Meta

Originally founded as Facebook Inc in 2004, Meta is a multi-national corporation incorporated in the United States. Its aim is to build technologies that help people connect, find communities, and grow businesses. Meta owns seven platforms:

---

132 Snap Inc Submission to Joint Select Committee on Social Media and Australian Society, Submission 40

Facebook

Facebook was Meta's first social media platform, released to the public in 2006. Today it has billions of monthly active users globally and is the third most visited website.

Instagram

Instagram is a photo and video sharing platform launched in 2010. It was purchased from its original owners by Facebook Inc in April 2012.

Messenger

Messenger, originally Facebook chat, is Meta's instant messaging app. It was launched in 2008 as part of Facebook and revamped as a separate application in 2015.

Threads

Threads is Meta's newest social media platform, launching in July 2023. It is described as a 'public conversation app,' running with a similar format to X (formerly Twitter).

WhatsApp

WhatsApp is a free instant messaging service, originally launched in 2009. It was purchased by Meta in 2014.

Workplace

Workplace is a platform specifically designed for businesses. It allows company staff to stay in touch via instant messaging, video conferences, posts, and more. It was launched by Meta in 2016.

Oculus VR

Oculus is an immersive virtual reality technology, purchased by Meta in 2014.

Age Restrictions

Meta restricts their platforms for individuals under age 13. This is achieved through an 'age screen' that requires individuals to provide their date of birth: those under 13 are not allowed to sign up.

Meta is working on artificial intelligence tools to better ensure users are the age they say they are. However, they note this technology is new and not as accurate as they would like.

Community Safety Standards

Meta's Community Safety Standards, are embedded in their website, and cover a range of policies specific to each of the company's platforms. These are available at: https://transparency.meta.com/en-gb/policies/.

Meta is understood to currently have 40,000 people working on developing and enforcing safety policies. The policies are developed through stakeholder consultation and designed to prohibit categories of harmful content from remaining on Meta's platforms, such as, child exploitation, adult sexual exploitation, violent and objectionable content, suicide and self-injury including eating disorders, bullying and harassment, hate speech and privacy violations.

Meta employs a strategy they call 'remove, reduce, inform' to manage content across Meta platforms: they remove content that violates their policies, reduce the reach of harmful content that does not violate policies, and inform users with additional context about that content to assist when deciding what to click, read or share.

Policy violating content is identified largely by user reporting mechanism. Meta also employs that they describe as 'proactive [AI] detection technology to identify and action harmful content before anyone reports it.'[133]

Example of safety policies and their enforcement – Facebook app

Content policies

Facebook outlines its content policies in its Community Standards, which applies to all its platforms. Broadly, Facebook prohibits or otherwise restricts content that promotes violent or criminal behaviour, poses a safety risk, or is "objectionable content", usually defined as hate speech, sexual content or graphic violence.

133 https://transparency.meta.com/en-gb/enforcement/detecting-violations/technology-detects-violations/

Violent, sexual, hateful, and fraudulent content are all prohibited outright. This includes content that pose an immediate safety risk, such as private identifying information that published maliciously (i.e., doxing). There are limited exceptions for newsworthy content, satirical content or matters expressed as opinion. These may be issued with a warning label or simply restricted rather than deleted. which is shared behind a warning label.

Meta also sets out policies around misinformation. The Content Policy states:

"We also remove content that is likely to directly contribute to interference with the functioning of political processes and certain highly deceptive manipulated media."[3]

Facebook enforces its policies with a mix of automated methods and human reviewers who train the automated systems over time. Users may also report posts they believe are in contravention of their content policies. Actions available to Facebook include deleting or restricting posts and accounts who contravene its rules. This information is set out in its Transparency Centre.

Facebook employs a "strike" system to restrict the accounts of users that violate its content policies. A first strike is usually only a warning, but further violations will attract a ban on the end-user from posting on their account. Bans can range from a one-day ban to a thirty-day ban. Accounts that repeatedly violate these rules will be disabled entirely. In addition, Meta has established an Oversight Board that reviews appeals for ban decisions.

User restricted access – Facebook groups

Facebook establishes on its platform Facebook Groups, whereby a user can establish a Group which selectively includes certain users. These groups may be made private so that only users who are a part of that group can access posts made within it. Groups are owned, managed and controlled by an administrator, who can be anyone with a user account on the website. This administrator has the power to:

- manage the group's membership, including admitting users and removing them
- remove posts in the group
- appoint moderators, who can assist with managing the group, and
- manage the group's settings, for example, changing the group name, cover photo or privacy settings.

The content posted by a group is subject to the same content policies detailed above. However, the groups feature allows for users to tailor posts for a specific use. This may include (but is not

exhaustive) to establish groups related to an interest (e.g., a hobby group), social circle, or educative group (e.g., a school page for which only students are admitted). Generally, the administrator will set out their own guidelines for what should be posted. For example, an administrator may create a page dedicated to fishing and dictate that all posts should be related to this topic and may remove posts or members who do not comply.

Transparency

Meta publishes quarterly reports to guarantee the transparency of their content moderation systems. They include: the Community Standards Enforcement Report[134], the Adversarial Threat Report (please see Attachment 1), and the Government Requests for User Data Report[135]. For example, 'the Community Standards Enforcement Report,' details the progress Meta's security teams have made with identifying and actioning reports of content that violates their policies. They claim that over 90% of content in a high-risk category, such as child exploitation content, is discovered and removed by machine leaning tools before Meta receives a user report flagging it.

Meta has over 400 safety partners worldwide to ensure their policies are complemented by industry expertise. This includes the Tech Coalition, described as 'an industry association dedicated solely to eradicating child sexual exploitation and abuse online.'[136]

Meta also employs in-app transparency information about the kinds of content being recommended to users through their recommender algorithm. For example, the 'why am I seeing this post?' feature allows users to tap on posts appearing on their feed to get information about why that post was recommended to them by the algorithm. They are then able to request they stop getting posts of this kind.[137]

134 https://transparency.meta.com/reports/community-standards-enforcement/

135 https://transparency.meta.com/reports/government-data-requests/country/

136 See https://www.technologycoalition.org/.

137 See https://about.fb.com/news/2019/03/why-am-i-seeing-this/#:~:text=%E2%80%9CWhy%20am%20I%20seeing%20this%20post%3F%E2%80%9D%2C%20which%20can,posts%20in%20your%20News%20Feed.

Settings that promote online safety for teenage users

By default, Meta places teenage users in the most restrictive content recommendation settings on Instagram and Facebook and applies stricter messaging default settings to prevent the receipt of messages from unknown persons and potentially suspicious accounts.

Default settings include:

- Setting teen accounts (between 13-18) on private.
- Teen profiles cannot be found in search engines on or off Meta platforms.
- Location tracking off.
- Adults are unable to message a teen who is not connected to them.
- Teens are prevented from messaging suspicious accounts (those who have been previously blocked or reported).
- Safety notices are issued to teen users if Meta flags that a person contacting them could be pursuing a potentially suspicious private interaction.
- Accounts flagged as potentially suspicious are unable to follow young people's accounts or see comments or comment themselves on their posts.
- Advertisers are only allowed to target user under 18 based on age and location metrics: data disclosing a teen's interests or interaction history on Meta platforms is unavailable to them.
- Warning labels are placed on sensitive content.

Adjustable Safety Settings

Meta's settings are adjustable to allow users to customise their experience. This allows users to tailor their experience to best fit their online safety needs. These settings include:

Blocking users

Blocking a user will prevent them from contacting you on Facebook Messenger or Instagram Direct Messenger. In addition, the blocked user can no longer tag you or invite you to events. Blocking is reciprocal: you will not be able to see their posts and they will not be able to see yours.

Unfollowing/unfriending users

When users unfollow someone, they will no longer see that user's posts on their feed. On Facebook, you will still be friends with someone you unfollow. If you choose to unfriend a user, they will not be notified.

Reporting content

Meta includes a link on nearly every piece of content that allows users to report abuse, bullying, harassment and other issues. Meta's global teams work 24 hours a day, 7 days a week to review reported content, and remove anything that violates their policies.

Restricting users

On Instagram, users can restrict another user. This means the restricted person will be unable to see if they are online or if they have read their messages. The restricted person's comments on their posts will be visible only to the user, and can then be approved, deleted or ignored.

Hidden words

Users can set the algorithm to filter certain harmful words and emojis.

Manage comments

Users can manage who is able to comment on their posts: the public, friends only, or only certain accounts.

Limits

Allows users to temporarily limit contact from anyone other than their close friends or recent followers.

Parental controls

Parents can view how much time their child spent on Instagram and Facebook set time limits.

Hide

Users can hide like counts on their own posts and or other users' posts to reduce social pressure.

Take a Break

Instagram's 'Take a Break' feature will advise users to take a break if they have been using the platform for a certain amount of time and suggest they set reminders to take more breaks in the future.

Recommender System Settings

Users can turn off the recommender system and switch to a feed that shows them content chronologically (in order of the date and time the content was posted).

Educational resources

Meta has a range of resources to assist parents to navigate online safety with their children. This includes the Parents Portal, a hub that includes information on social media safety, and a means of connecting parents with outside online safety organisations worldwide. In Australia specifically, Meta collaborated with ReachOut to develop the ***'Parents Guide to Instagram'*** to support parents in understanding Instagram's safety tools.

Meta — Public commentary

Submission to the House Select Committee on Social Media and Online Safety

Meta made submissions in 2022, to the House Select Committee on Social Media and Online Safety. The 'policies, enforcement techniques, tools, products, resources and partnership' integral to facilitating safety online for Meta platform users were outlined in detail.[138] The information provided in this regard emulates the information provided above surrounding their later submission to the Joint Select Committee on Social Media and Australian Society.

---

138 Meta, Submission No 49 to *House Select Committee on Social Media and Online Safety* (January 2022) 2.

Meta claimed from the outset, 'Industry, government and the community all have a role to play in working towards online safety.'[139] Meta spoke of its continual support and adherence to regulatory developments by Australian, as evidenced by their status as the first company to endorse the ESafety Commissioner's Safety by Design Guidelines.[140] However, the company warned Australian policy and law makers against the increase in regulatory measures within the Australian jurisdiction, by stating:

> Given the recent history of active rulemaking, we suggest therefore that this Committee should focus its attention on whether the slew of regulations are effective or necessary.
>
> Policymaker should be alive to the risk of overlapping, duplicative or inconsistent rules across different laws. Indeed, many of the online safety-related laws and regulations that have already been passed by Parliament are yet to be implemented. Policymaker will be able to develop more effective regulation if there is consideration given to properly understanding the effectiveness of existing regulation first.[141]

Speaking to the global nature of the Internet and other regulatory goals of various nations, Meta states:

> The overall regulatory approach taken by Australia needs to be viewed in the context of a global contest of competing visions of the internet.

Other countries look to Australia, and it is important to consider whether Australian regulation sets an example which encourages a liberal, open and democratic approach to the internet, or an internet that is more closed, tightly controlled and fragmented.'[142]

These sentiments were reinforced throughout the submission, whilst also emphasising the work Meta had done with respect to safety and protection of all users.

---

139 See ibid.
140 Ibid 4, 88.
141 Ibid 4-5.
142 Ibid 5.

Submission to the Joint Select Committee on Social Media and Australian Society — 2024

Meta suggested at the outset that the suite of applications within their control are integral to everyday communication between friends, families, organisations, and communities, thus, their obligation to 'be responsive to community concerns, and to promote transparency and accountability' is paramount.[143]

Meta spoke of being a member of an array of Online Safety Partnerships. Among these is the Tech Coalition 'a global alliance of technology companies that work together to drive critical advances in technology and adoption of best practices for keeping children safe online.'[144] Meta's collaboration with the Tech Coalition has allowed it to establish itself as a founding member of the Lantern Program, which aims to facilitate collaboration with technology companies for the purposes of identifying various accounts and behaviours which are in violation of Child Safety Policies.[145] An Australian Online Safety Advisory Committee has been established and has more recently contributed to endeavours towards youth safety online as initiated by PROJECT ROCKIT, ReachOut, Kids Helpline and ACCCE and the Butterfly Foundation.[146]

Policies, such as the Facebook Community Standards and Instagram Community Guidelines, have been produced with feedback from the community and the submissions of experts in 'technology, public safety, child safety and human rights.'[147] Meta contended that such policies are amenable to align with advances both in the online and offline world.[148] Specific approaches have been developed and consolidated with respect to youth online namely, mental health and wellbeing, eating disorder content, suicide and self-injury, sextortion, hate speech, violent and extremist content and misinformation.[149] Meta has provided detailed strategies for the targeting of each of these issues per their submissions.[150]

---

143 Meta, Submission No 46 to *Joint Select Committee on Social Media and Australian Society* (June 2024) 2.
144 Ibid 4.
145 Ibid 12.
146 Ibid 12–13.
147 Ibid 10.
148 See ibid.
149 Meta, Submission No 46 to *Joint Select Committee on Social Media and Australian Society,* Parliament of Australia (June 2024) 21-37.
150 Ibid 21–37.

Meta also referred to its implementation of internal safety mechanisms, community guidelines, transparency reports and the extensive undertaking of safety associated endeavours.

TikTok

The Examination was assisted by Ella Woods- Joyce, Director of Public Policy, TikTok AUNZ; Amelia Crawford, Legal Counsel, TikTok, AUNZ and Tom Fardoulys, Public Policy Manager, TikTok AUNZ.

A general outline, based on materials sourced from TikTok's website, of their practices and policies follows.

What is TikTok?

TikTok is a social media platform for creating and sharing short videos. TikTok has a minimum user age of 13 years. Users can either sign up using their Facebook, Instagram, X, or email account.

The search tool allows users to view other videos. Users can also view content under the trending hashtags on the 'For You' page.

Trending hashtags allow users to view content that is currently popular, and to upload their own video to that trend using the same hashtag.

TikTok Wellbeing and Privacy Measures[151]

- An hour daily screen time limit will be automatically set for every account belonging to a user under age 18. If users reach the limit they will be prompted to enter a passcode in order to continue watching, requiring them to make an active decision to extend that time.
- Default privacy settings which includes setting the accounts of users aged 13-15 to private by default.
- Restricting the comments on posts of users in this age range to 'friends' or 'no one'.

[151] Please note: this information is based on public websites with content about TikTok, and additional measures may have been established since these were put in place.

- Disabling the download video feature for users under the age of 16.
- Restricting direct messaging and hosting live streams to accounts 16 and over.
- Restricting the buying, sending, and receiving of virtual gifts to users below 18.

Additional features have also been added to the Family Pairing options, including custom daily screen time limits, screen time dashboard, and mute notification options that allow parents to set a schedule to mute notifications for their teenager.[152]

Policies and procedures

A number of TikTok policies related to user safety and harm minimisation measures were considered.

TikTok — Public commentary

TikTok's submission to the Joint Select Committee on Social Media and Australian Society set out advice provided by the company on a range of matters related to the Terms of Reference including:

- Community Guidelines and Enforcement mechanisms (see from p. 2)
- Age assurance (position, and mechanisms, see p. 3)
- Age appropriate settings and controls (see p. 3)
- Approaches to youth safety (see p.4)
- TikTok's performance in relation to detecting child sexual exploitation and abuse, as reported by the eSafety Commissioner's Basic Online Safety Expectations transparency report from October 2023 (see p. 5)
- TikTok's recommendation system (see p. 8)

[152] https://www.webwise.ie/parents/explained-tiktok/#:~:text=What%20is%20TikTok%3F-,What%20is%20TikTok%3F,share%20them%20across%20a%20community.

Chapter 10: What would an exempt social media service look like?

The proposed legislative model would impose duties on social media service providers. The duties would not apply to providers of exempt social media services. Although classes of exempt social media service could be specified in the legislation, as appears from some of the international examples considered — it is suggested that exemption be a matter for ministerial determination or legislative instrument, including regulations. It is reasonable, however, to consider what kinds of social media services might be exempted.

A leading example would be a social media service provided by public authorities for a range of purposes, including the provision of online information, advice and counselling.

A general social media service used in an educational setting, e.g. by a teacher controlling access by students, in a support group setting for minors, a children's club or society where access is limited to members and to interaction between members and subject to control by an adult administrator. Examples may be multiplied of such uses of social media which are child safe and beneficial and which should not be precluded by age based restrictions on access. The Examination was told of the benefits of online social interaction for particular groups of children e.g. First Peoples' children in remote communities and others. Social media services beneficially designed to overcome social isolation and to encourage supportive interactions for children and controlled by adult administrators, precluding access by or to the wider universe of users, would be obvious candidates for exemption.

There are many examples of educational applications with social functions but not all of which are connected with social media. The examples that follow have been prepared by officers of the South Australian Department for Education. They are digital platforms and apps used in South Australian public schools. Some of them operate in a 'closed environment' (e.g. Class Dojo) in that they are only accessible within the school community.

The list follows:

EdTech applications with social functions

1. Adobe Express - collaboration

- **Description**: A tool for creating visually engaging content, including graphics, videos, and webpages, with collaborative features.

- **Functions**:
    - Content creation and editing
    - Collaboration on projects
    - Sharing on social media platforms
    - Integration with other Adobe tools

2. Canva for Education - collaboration

- **Description**: A design platform tailored for educational use, enabling students and teachers to create and collaborate on visually appealing projects.
- **Functions**:
    - Collaborative design in real-time
    - Access to educational templates
    - Integration with Google Classroom
    - Sharing on social media or direct publishing

3. Class Dojo

- **Description**: A classroom communication app connecting teachers, students, and parents, focused on student behaviour and engagement.
- **Functions**:
    - Facebook-like feeds
    - Behaviour tracking and reporting
    - Communication with parents
    - Digital portfolios for students
    - Classroom announcements (no direct social media integration)

4. **ClickView**

- **Description**: An educational video content platform providing access to curriculum-aligned videos and interactive resources.
- **Functions**:
    - Video streaming and sharing
    - Interactive video features
    - Content creation and curation
    - Integration with LMS (no direct social media features)

5. **Compass**

- **Description**: A school management platform covering attendance, reporting, and communication between teachers, students, and parents.
- **Functions**:
    - Attendance tracking and reporting
    - Parent-teacher communication
    - Assessment and progress reporting (teacher – student feedback)
    - Calendar and event management (no social media features)

6. **CoSpaces (collaboration)**

- **Description**: A platform for creating and exploring 3D virtual environments, with collaborative tools for educational projects.
- **Functions**:
    - 3D creation and coding
    - Collaborative building and sharing
    - Integration with VR headsets

- Sharing projects within the platform (limited social media sharing)

7. Desmos Classroom

- **Description**: An interactive platform for exploring mathematical concepts through visual and interactive tools.
- **Functions**:
  - Interactive graphing calculator
  - Collaborative math activities
  - Classroom management tools
  - Sharing of activities (no direct social media integration)

8. Edmodo

- **Description**: A social learning network connecting teachers, students, and parents, facilitating classroom communication and resource sharing.
- **Functions**:
  - Classroom communication and announcements
  - Assignment and quiz management
  - Resource sharing and collaboration
  - Integration with social media platforms

9. Edublogs

- **Description**: A blogging platform designed for educators and students, enabling them to create and share content within a controlled environment.
- **Functions**:
  - Blog creation and customization
  - Commenting and collaboration

- Privacy controls for student safety
- Integration with social media for sharing

10. Flip

- **Description**: A video discussion platform where students and teachers can engage in interactive conversations.
- **Functions**:
  - Video recording and sharing
  - Collaborative video discussions
  - Integration with LMS platforms
  - Social media sharing options available

11. Frog

- **Description**: A learning management system (LMS) offering a comprehensive set of tools for managing and delivering educational content.
- **Functions**:
  - Course and content management
  - Collaboration on assignments
  - Communication tools for students and teachers
  - Social sharing through integrated features

12. Google Apps - Google Workspace for Education

- **Description**: A suite of productivity and collaboration tools tailored for educational institutions, including Google Docs, Sheets, Slides, and Classroom.
- **Functions**:
  - Document collaboration in real-time

- Classroom management and assignments
- Email and calendar integration
- Sharing on Google platforms (some social media integration via sharing links)

13. Kahoot

- **Description**: A game-based learning platform where students can participate in quizzes and interactive lessons.
- **Functions**:
  - Quiz creation and participation
  - Real-time collaboration and competition
  - Sharing results and quizzes on social media
  - Integration with classroom tools

14. Kai's Clan Classroom (Chat function can be turned off by teacher) - coding robots

- **Description**: A collaborative coding platform where students can program robots in a virtual or physical environment.
- **Functions**:
  - Coding and robotics programming
  - Classroom collaboration on coding projects
  - Chat function for communication (can be disabled)
  - Integration with other educational platforms (limited social media features)

15. Kidblog

- **Description**: A safe blogging platform for students, allowing them to publish content and collaborate within a secure environment.
- **Functions**:
    - Blog creation and management
    - Commenting and peer collaboration
    - Teacher moderation and control
    - Integration with social media for sharing blogs

16. Kidspiration/Inspiration (mind mapping collaboration)

- **Description**: Tools for visual thinking and mind mapping, helping students to organize and express their ideas.
- **Functions**:
    - Mind mapping and diagram creation
    - Collaboration on visual projects
    - Integration with other educational tools
    - Sharing projects within the platform (limited social media features)

17. Learning Management Systems (Frog, Day Map, Canvas, Moodle)

- **Description**: Platforms designed for managing, delivering, and tracking educational content and student progress.
- **Functions**:
    - Course creation and content delivery
    - Assignment and assessment management
    - Student progress tracking

- Some systems offer integration with social media for content sharing

18. Lucidchart - collaboration free for education use

- **Description**: A web-based diagramming tool that supports collaborative creation of flowcharts, diagrams, and mind maps.
- **Functions**:
  - Collaborative diagram creation
  - Integration with Google Workspace and other platforms
  - Sharing diagrams via links or social media
  - Free access for educational use

19. Lumio (collaborative learning for SmartBoard)

- **Description**: A digital learning tool that integrates with SmartBoards to create interactive lessons and collaborative activities.
- **Functions**:
  - Interactive lesson creation
  - Real-time student collaboration
  - Integration with SmartBoard tools
  - Sharing lessons within the platform (no direct social media features)

20. Mathletics (no chat as such but matched and compete with other students around the world with the same ability level)

- **Description**: An online math platform offering personalized learning, practice, and competition among students worldwide.
- **Functions**:
  - Personalized math practice and tutorials

- Global competitions with peers
- Progress tracking and reporting
- Limited social interaction (no chat, competition-based)

21. Mentimeter

- **Description**: An interactive presentation tool that allows real-time audience participation through polls, quizzes, and Q&A sessions.
- **Functions**:
  - Polling and quiz creation
  - Real-time audience interaction
  - Data visualization and reporting
  - Sharing results on social media

22. Microsoft Apps - Microsoft 365 Educational licensed apps

- **Description**: A suite of productivity and collaboration tools from Microsoft, including Word, Excel, PowerPoint, and Teams.
- **Functions**:
  - Document creation and collaboration
  - Classroom management with Teams
  - Email and calendar integration
  - Sharing on Microsoft platforms (limited social media integration)

23. Minecraft / MinecraftEDU

- **Description**: An educational version of Minecraft that allows students to collaborate and learn through creative building and problem-solving.

- **Functions**:
    - World-building and exploration
    - Collaborative learning experiences
    - Coding and STEM integration
    - Sharing projects within the Minecraft community (limited social media sharing)

24. Mirro - free for education use

- **Description**: An interactive whiteboard platform that supports real-time collaboration and brainstorming.
- **Functions**:
    - Collaborative whiteboarding and brainstorming
    - Integration with educational tools
    - Sharing boards and projects
    - Free access for educational use (limited social media integration)

25. Mondly (VR language learning)

- **Description**: A language-learning app that uses virtual reality (VR) to immerse students in interactive language experiences.
- **Functions**:
    - VR-based language lessons
    - Interactive language practice
    - Progress tracking
    - Limited sharing features within the app

26. Padlet

- **Description**: An online bulletin board that enables students and teachers to post notes, images, and links in a collaborative space.
- **Functions**:
    - Collaborative note posting
    - Anonymous participation options
    - Integration with other classroom tools
    - Sharing boards via links or on social media

27. Quizziz

- **Description**: A quiz-based learning platform that allows students to participate in interactive quizzes and assessments.
- **Functions**:
    - Quiz creation and participation
    - Real-time feedback and results
    - Collaborative learning modes
    - Sharing quizzes on social media platforms

28. Roblox

- **Description**: A gaming platform where users can create and play games, with educational potential in coding and game design.
- **Functions**:
    - Game creation and coding
    - Collaboration within the Roblox community
    - Educational use in coding and design

- Sharing games and projects within the platform (limited social media features)

29. Schoology

- **Description**: A learning management system (LMS) that offers tools for course management, assignments, and communication.
- **Functions**:
  - Course creation and content delivery
  - Assignment and grade management
  - Communication tools for students and teachers
  - Integration with social media for content sharing

30. Seesaw

- **Description**: A student-driven digital portfolio platform that allows students to document and share their learning.
- **Functions**:
  - Facebook-like feeds
  - Digital portfolio creation
  - Student-teacher-parent communication
  - Collaboration on assignments
  - Sharing portfolios with parents (limited social media sharing)

31. SEQTA

- **Description**: A comprehensive school management system that supports attendance, reporting, and communication.

- **Functions**:
    - Attendance tracking and reporting
    - Academic and pastoral care management
    - Parent-teacher communication
    - No direct social media integration

32. Slido

- **Description**: An audience interaction platform that allows for real-time polling, Q&A, and feedback during presentations.
- **Functions**:
    - Poll creation and management
    - Live Q&A sessions
    - Data collection and analysis
    - Sharing results via social media

33. Stile

- **Description**: A science-focused learning platform offering interactive lessons, quizzes, and activities aligned with curriculum standards.
- **Functions**:
    - Interactive lesson delivery
    - Quizzes and assessments
    - Real-time feedback and progress tracking
    - Integration with other classroom tools (no direct social media features)

34. Storify

- **Description**: A storytelling platform that allows users to curate social media content into a cohesive narrative.
- **Functions**:
    - Content curation from social media
    - Story creation and editing
    - Sharing stories on social media platforms
    - Collaboration on storytelling projects

35. Stormboard

- **Description**: A collaborative online whiteboard tool that supports brainstorming and project management.
- **Functions**:
    - Brainstorming and ideation
    - Real-time collaboration
    - Project management and task tracking
    - Sharing boards and projects (limited social media integration)

36. Thinglink - collaboration

- **Description**: An interactive media platform that allows users to create and share interactive images, videos, and VR experiences.
- **Functions**:
    - Interactive media creation
    - Collaboration on projects
    - Integration with VR and AR tools

- Sharing on social media platforms

37. TinkerCad

- **Description**: A web-based 3D design and modeling tool, particularly useful for STEM education and coding projects.
- **Functions**:
  - 3D modeling and design
  - Coding and STEM integration
  - Collaboration on projects
  - Sharing designs within the platform (limited social media features)

38. Vimeo

- **Description**: A video-sharing platform with advanced privacy controls, commonly used for educational content.
- **Functions**:
  - Video hosting and sharing
  - Commenting and collaboration (if enabled)
  - Advanced privacy settings
  - Sharing videos on social media platforms

39. VRTY (create VR environments and share with others)

- **Description**: A platform for creating and sharing virtual reality (VR) environments, particularly suited for educational use.
- **Functions**:
  - VR environment creation
  - Collaboration on VR projects

- Integration with educational tools
- Sharing within the platform (limited social media features)

40. Wakelet

- **Description**: A content curation platform that allows users to save, organize, and share content from the web.
- **Functions**:
  - Content curation and organization
  - Collaboration on collections
  - Sharing collections via social media
  - Integration with classroom tools

41. Weebly/Wix website builders

- **Description**: Website creation platforms that offer drag-and-drop tools for building websites, with educational plans available.
- **Functions**:
  - Website creation and customization
  - Collaboration on website projects
  - Integration with third-party tools
  - Sharing websites on social media

42. YouTube

- **Description**: A video-sharing platform where users can upload, share, and view videos, with broad educational applications.
- **Functions**:
  - Video creation and editing

- Channel management and subscriptions
- Commenting and community engagement
- Broad social media sharing options

Comment

Plainly, those applications which allow for interaction beyond the class group using them, if not controlled by an adult administrator, e.g. a teacher, might have a greater difficulty in securing exemption status than those which do not.

South Australian Commissioner for Children and Young People

The South Australian Commissioner for Children and Young People did provide some information on what platforms might be exempted from the proposed ban. She referred to the views of young people in Years 10 to 12 who are members of the South Australian Student Representative Council. They raised concerns about the broad definition of 'social media service' in the *Online Safety Act* and the implications of a ban on platforms they use for their education, employment and social life. They identified several platforms that they contended should be exempt from the ban based on where and how they are used and their perceptions of potential harms.

WhatsApp, Spotify and YouTube were apps which it was said should be exempt. The Commissioner was told that they don't usually cause too much of an issue and it was a way to connect with the world. Absent that connection, 'kids would just feel isolated and it will encourage sneakiness and lying, not to mention they are used for learning at schools'.

It was also argued that Messaging apps like Messenger and WhatsApp should be exempt because of their importance as communication tools and the fact that they have in place a range of safeguards for children. If Internet-based messaging apps are caught up in the ban they would not be able to have group chats with people who have different types of phones, i.e.. iPhone versus Android.

WhatsApp messaging can only be exchanged with those who have your phone number. Kids Messenger was already managed by parents who were notified. In order to create new friends

on Kids Messenger, parental approval was necessary. The parents would create a children's account under their Facebook.

Young people to whom the Commissioner spoke highlighted that Spotify and Musescore should be exempt because they are used at school. It helps focus. It is particularly important for music students and also for neuro-divergent students.

Young people were also said to use YouTube and Pinterest for a range of educational and creative purposes at school and outside of school. Those platforms should be exempt because they were relatively unproblematic.

Microsoft Teams, Google Classrooms, Daymap and Seqta were cited as platforms which are used in schools to connect students with each other, with staff and with information.

There was reference by some young people to concerns about negative experiences on certain platforms, particularly at a young age. Their responses were said by the Commissioner to highlight the importance of listening to children and young people about their use of different platforms and providing them with information about the ban and affected platforms.

The South Australian Deputy Chief Psychiatrist, Dr Melanie Turner, said that overall the largest issue with social media was that it allowed children and adolescents access to a volume of information that they were not developed mentally ready to understand or interpret. Before exposure to a large amount of data on social media, children's exposure to sights, sounds and experiences were those offered by their families, friends and schools. If no one in their circle talked about self-harming they were not exposed to it. Online there could be exposure to self-harming. A child so exposed would experience something in isolation away from context, support and an adult framework to interpret it. There would not be a safety net or filter by way of a parent or career to intercept, realign or reshape the experience. The spaces that were most unsafe from the point of view of the Deputy Chief Psychiatrist were large user programs where the child would be able to view content by anyone with no filters. Even if a child did not make content, they were exposed as a vulnerable user. The Deputy Chief Psychiatrist identified sites which she contended were unsafe and should not accessible ideally to those under 16, but under 14 if that were the limit. She listed TikTok, YouTube, Instagram, Snapchat, Facebook,

WhatsApp and Kik. She also suggested that Discord can be a problem for open chat settings as well although most gamers use the VOIP to talk during gaming and to also instantly message.

Comment

The category of potential exempt social media services is not closed by reference to the categories discussed in the earlier part of this chapter. It would be for the Regulator to develop and promulgate guidelines for providers of social media services seeking exempt status for their service. This would necessarily be an interactive process and would require access on the part of the Regulator to relevant technical expertise and advice. This might in part be done through cooperative arrangements with the Office of the eSafety Commissioner.

Chapter 11: Organisational characteristics and location of social media ownership and control in Australia — availability to State regulation

The great bulk of social media service owners and providers are corporations outside Australia, They would fall into the category of 'foreign corporations' for the purposes of the Commonwealth's constitutional power to make laws with respect to foreign corporations and trading and financial corporations formed within Australia.

The table which follows has been derived from free publicly available materials. It does not pretend to be exhaustive, but covers a number of familiar social media services.

Table of Social Media Service Providers in Australia

Social Media Service	Parent Company	Contractual Service Provider to Users in Australia
Addchat Available at: https://addchat.animaapp.io/ Terms and Conditions Available at: https://addchat.animaapp.io/terms	Addchat Inc. (Delaware, USA)	Addchat Inc. (Delaware, USA)
Bluesky Terms of Service Available at: https://bsky.app/	Bluesky Social Public Benefit Corporation (Delaware, USA)	Bluesky Social Public Benefit Corporation (Delaware, USA)
Bumble (including Bumble for Friends) Terms of Service Available at: https://bumble.com/en_au/	Bumble Inc (Delaware, USA)	"The Bumble Group" Bumble Holding Limited (UK)

		Bumble Trading LLC (Delaware, USA) Bumble Inc (Delaware, USA) Social Online Payments Limited (Republic of Ireland) Social Online Payments LLC (Delaware, USA)
Discord Terms of Service	Discord Inc (Delaware, USA)	Discord Inc (Delaware, USA)
Facebook (including Facebook live, Messenger, Messenger kids) Terms of Service	Meta Platforms Incorporated (Delaware, USA)	Meta Platforms Incorporated (Delaware, USA)
Flickr Terms and Conditions of Use	SmugMug Incorporated (USA)	Flickr Incorporated (Delaware, USA)
Foursquare City Guide Terms of Use	Foursquare Labs, Inc (Delaware, USA)	Foursquare Labs, Inc (Delaware, USA)

Foursquare Swarm Terms of Use	Foursquare Labs, Inc (Delaware, USA)	Foursquare Labs, Inc (Delaware, USA)
Grindr Terms of Service	Grindr Group LLC (Delaware, USA)	Grindr LLC (California, USA)
Happn Terms of Service	Happn (France)	Happn (France)
Imgur Terms of Service	MediaLab.Ai Incorporated (Delaware, USA)	MediaLab.Ai Incorporated (Delaware, USA)
Instagram (including Reels and Threads) Terms of Use	Meta Platforms Incorporated (Delaware, USA)	Meta Platforms Incorporated (Delaware, USA)
Kick Terms of Service	Easygo Entertainment Pty Ltd (Australia)	Kick Streaming Pty Ltd (Australia)
Lego Life	Kirkbi A/S (Denmark)	Lego System A/S (Denmark)

Terms of Use		
Linkedin User Agreement	Microsoft Corporation (Washington, USA)	LinkedIn Corporation (Delaware, USA)
LiveMe Terms of Service	Cheetah Mobile Incorporated (Cayman Islands)	Hong Kong LiveMe Corporation Limited (Hong Kong)
Mastodon	Decentralised (no corporation or person operating service) Mastodon, Incorporated (Germany non-profit LLC)	Decentralised (no corporation or person operating service) Mastodon, Incorporated (Germany non-profit LLC)
Melon Terms of Use	Melon Inc (Delaware, USA)	Melon Inc (Delaware, USA)
Microsoft Teams (including Viva Engage) Services Agreement	Microsoft Corporation (Washington, USA)	Free services Microsoft Ireland Operations Limited (Republic of Ireland) Paid services Microsoft Pty Ltd
OmeTV	Bad Kitty's Dad LDA (Portugal)	Bad Kitty's Dad LDA (Portugal)

Terms of Service		
Patreon Terms of Use	Patreon Incorporated (Delaware, USA)	Patreon Incorporated (Delaware, USA)
Pinterest Terms of Service	Pinterest Inc (Delaware, USA)	Pinterest Europe Ltd (Republic of Ireland)
Reddit User Agreement	Reddit Inc (Delaware, USA)	Reddit Inc (Delaware, USA)
Skype Services Agreement	Microsoft Corporation (Washington, USA)	Free services Microsoft Corporation (Washington, USA) Paid services Skype Communications (Luxembourg)
Snapchat Terms of Service	Snap Inc (Delaware, USA)	Free services Snap Group Limited (United Kingdom) Paid services Snap Group Limited Singapore Branch (Singapore)

Steam	Valve Corporation (Washington, USA)	Valve Corporation (Washington, USA)
Telegram Terms of Service	Telegram Messenger Inc (British Virgin Islands)	
TikTok Terms of Service	ByteDance Ltd (Cayman Islands)	TikTok Pte Limited (Singapore)
Tinder Terms of Use	Match Group Inc (Texas, USA)	Tinder LLC (Texas, USA)
Twitch Terms of Service	Amazon.com Inc (Delaware, USA)	Twitch Interactive Inc. (Delaware, USA)
Vimeo Terms of Service	Vimeo.com Incorporated (Delaware, USA)	Vimeo.com Incorporated (Delaware, USA)
Wattpad Terms of Service	Naver Corporation (South Korea)	Wattpad Corporation (Ontario, Canada)

Wechat Terms of Service	Tencent Holdings Ltd (China)	WeChat International Pte. Ltd (Singapore)
WhatsApp Terms of Service	Meta Platforms Incorporated (Delaware, USA)	WhatsApp LLC (Delaware, USA)
Wizz Terms and Conditions	Voodoo SAS (France)	WIZZ SAS (France)
x (formerly known as Twitter) Terms of Service	X Corp. (Nevada, USA)	Free services X Corp. (Nevada, USA) Paid services Twitter Global LLC (Delaware, USA)
YouNow Terms of Use	YouNow Media LLC (Delaware, USA)	YouNow Media LLC (Delaware, USA)
YouTube (including YouTube Kids, YouTube Music, YouTube Premium, YouTube TV and YouTube Shorts) Terms of Service	Google LLC (Delaware, USA)	Free services Google LLC (Delaware, USA) Paid services

		Google Ireland Limited (Republic of Ireland)
Yubo Terms of Service	Twelve-App SAS (France)	Twelve-App SAS (France)

Comment

There is a need for a South Australian law to have a territorial link with South Australia. However, that does not mean that a South Australian law can apply only to providers based in South Australia. A generic definition of a 'social media service provider' can be framed having regard analogously to the UK *Online Safety* Act, by reference to any provider whose social media service is accessible to users within the State of South Australia. It would not be necessary for the valid operation of a South Australian law that it apply only to providers based in Australia.

It should be noted that any foreign corporation carrying on business in Australia must be registered under Div 2 of Ch 5B of the *Corporations Act 2001* (Cth) and must have at least one local agent.

As indicated later in this Report, it is uncontroversial that a valid State law can apply to a foreign corporation carrying on business or engaging in other activity within the State — which in this case would include the provision of access to social media services by people living in South Australia.

Chapter 12: Convention on the Rights of the Child — implications for regulation of access to social media by minors

This Examination would not be complete without reference to the *Convention on the Rights of the Child*. Australia is a party to the *Convention on the Rights of the Child*, which entered into force on 2 September 1990.[153] Section 24 of the *Online Safety Act* refers to the *Convention on the Rights of the Child* and provides:

> (1) The Commissioner must, as appropriate, have regard to the Convention on the Rights of the Child in the performance of functions:
>
> (a) conferred by or under this Act; and
>
> (b) in relation to Australian children.
>
> (2) Subsection (1) does not limit the matters to which the Commissioner may have regard.

The recitals to the Convention referred to the Universal Declaration of Human Rights[154] and the proclamation in that Declaration that 'childhood is entitled to special care and assistance.' The term 'child' in the Convention was defined in Art 1 as 'every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.'

Relevantly to the present Examination, Art 12 provides:

> ***Article 12***
>
> 1. States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

Article 12(2) is not material for present purposes.

Article 13 provides:

> ***Article 13***
>
> 1. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds,

---

153 *Convention on the Rights of the Child*, opened for signature 20 November 1989 (entered into force 2 September 1990).

154 *Universal Declaration of Human Rights*, GA Res 217A, UN GAOR UN Doc A/810 (10 December 1948).

regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

2. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others; or

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Article 17 provides:

Article 17

States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health. To this end, States Parties shall:

(a) Encourage the mass media to disseminate information and material of social and cultural benefit to the child and in accordance with the spirit of article 29;

(b) Encourage international co-operation in the production, exchange and dissemination of such information and material from a diversity of cultural, national and international sources;

(c) Encourage the production and dissemination of children's books;

(d) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous;

(e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

2021 saw the publication, by the United Nations Committee on the Rights of the Child, of General Comment No 25 on 'Children's Rights in Relation to the Digital Environment'. The General Comment took the form of an explanation by the Committee of how States Parties should implement the Convention in relation to the digital environment and provided guidance on relevant legislative policy and other measures to ensure full compliance with States obligations under the Convention an optional protocols thereto.

The Committee enunciated four general principles:

(1) Non-discrimination

(2) The best interests of the child

(3) The right to life, survival and development

(4) Respect for the views of the child

In relation to the 'best interests of the child', the General Comment said:

> States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.[155]

Consideration of the best interests of the child should have regard to children's rights, including their rights to seek, receive and impart information, to be protected from harm and to have their own views given weight.

In relation to the 'rights to live, survival and development', it was said that opportunities provided by the digital environment play an increasingly crucial role in children's development and may be vital for a child's life and survival, especially in situations of crisis. The need for appropriate measures to protect children from the risks and online harms was referred to.

Then it was said:

> 15. The use of digital devices should not be harmful, nor should it be a substitute for in-person interactions among children or between children and parents or caregivers. States parties should pay specific attention to the effects of technology in the earliest years of life, when brain plasticity is maximal and the social environment, in particular relationships with parents and caregivers, is crucial to shaping children's cognitive, emotional and social development. In the early years, precautions may be required, depending on the design, purpose and uses of technologies. Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development especially during the critical neurological growth spurts of early childhood and adolescence.[156]

Respect for the views of the child was urged. The Comment referred to reports from children that the digital environment 'afforded them crucial opportunities for their voices to be heard in matters that affected them.' The use of such technologies could help to realise children's participation at the local, national and international levels. State parties were encouraged to promote awareness of and access to digital means for children to express their views and to offer training and support for children to participate on an equal basis with adults anonymously where needed so they could be effective advocates for their rights individually and as a group.

---

155 General Comment No 25 [12].

156 General Comment No 25 [15].

Consultation about developing legislation policies, programs, services and training on children's rights was also encouraged. States were encouraged to ensure that 'digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services.'[157]

It was also stated that:

> States parties should implement measures that protect children from risks, including cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, ensure the investigation of such crimes and provide remedy and support for children who are victims. They should also address the needs of children in disadvantaged or vulnerable situations, including by providing child-friendly information that is, when necessary, translated into relevant minority languages.[158]

As to civil rights and freedoms and access to information, the General Comment stated that:

> 51. States parties should provide and support the creation of age-appropriate and empowering digital content for children in accordance with children's evolving capacities and ensure that children have access to a wide diversity of information, including information held by public bodies, about culture, sports, the arts, health, civil and political affairs and children's rights.

In relation to freedom of expression, Art 59 of the Geneal Comment stated:

> 59. `Any restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate …

It was asserted that States parties should ensure that their laws, regulations and policies protect children's rights to participate in organisations that operate partially or exclusively in the digital environment. It was said that no restrictions may be placed on the exercise by children of their right to freedom of association and peaceful assembly in the digital environment other than those that are lawful, necessary and proportionate.

States parties were encouraged to use digital technologies to promote healthy lifestyles, including physical and social activity.[159] Digital technologies were said to offer multiple opportunities for children to improve their health and wellbeing when balanced with their need for rest, exercise and direction interaction with their peers, families and communities. States parties, it was suggested, should develop guidance for children, parents, caregivers and

---

157 General Comment No 25 [17].
158 General Comment No 25 [25].
159 General Comment No 25 [97].

educators regarding the importance of a healthy balance of digital and non-digital activities and sufficient rest.

As to education, leisure and cultural activities, the General Comment asserted that the digital environment can greatly enable and enhance children's access to high quality inclusive education, including reliable resources for formal, non-formal, informal, peer-to-peer and self-directed learning.

The point was made that for children who are not physically present in school or for those who live in remote areas or in disadvantaged or vulnerable situations, digital education or technology can enable distance or mobile learning. It was proposed that State parties should ensure that there is proper infrastructure in place to enable access for all children to the basic utilities necessary for distance learning, including access to devices, electricity, connectivity, educational materials and professional support.

The right to culture, leisure and play, was directed to the beneficial use of digital technologies in this regard.

The approach taken in the General Comment to the obligation of State parties under the *Convention on the Rights of the Child* was reflected in a meeting with Ms Helen Connolly, the Commissioner for Children and Young People in South Australia.

Comment

The *Convention on the Rights of the Child* does not constrain the law-making power of the South Australian Parliament relevant to a proposed ban. International Conventions do not have direct effect in Australia as municipal law unless given effect by legislation. There is, in any event, considerable room for parties to the *Convention* to move in their assessment of the balance between rights and freedoms of children and the protective measures necessary to prevent them from exposure to harm.

The views of the eSafety Youth Council

It is appropriate in this context to refer to views submitted to the Examination by the eSafety Youth Council. In a meeting held on 8 August 2024 members of the eSafety Youth Council discussed with the Examiner:

- Risks and benefits of social media access and use, particularly in relation to LGBTQIA+ teens, First Nation teens and young people with a disability.
- The scrolling aspect of some social media and its impact on attention spans and its addictiveness for those under 14.
- The importance of messaging apps for communication and social connection between teens.

Some further written submissions were received from two members of the eSafety Youth Council which it is useful to reproduce in full.

> eSafety **Youth Council**
>
> Additional Submissions to the Honourable Robert French AC
>
> [a **16 year OLD]**
>
> **…**
>
> **1. Legislative Action at the State Level:**
>
> Define Scope and Enforcement: Clearly outline what constitutes "social media" and specify the targeted age group. Enforcement methods should be detailed, such as fines for non-compliant social media companies, similar to the Online Safety Act 2021.
>
> Public Support: To gain public backing, especially from parents and teachers, draw parallels between social media and activities like alcohol consumption or driving—both of which require responsible use. This approach could also resonate with many young people.
>
> **2. Existing Legislative Landscape:**
>
> Gap in the Online Safety Act 2021: The current Online Safety Act mainly addresses cyberbullying and image-based abuse, but it doesn't cover violent or misleading content. This gap could motivate a push for stricter regulations.
>
> **3. Effective Enforcement Using Existing Technology:**
>
> Age Assurance Technology: Use age verification through official documents like driver's licences or passports, verified by software. To address privacy concerns, the government could limit the data collected to the minimum necessary, reducing the impact of potential data breaches.
>
> **4. A matter of utmost importance that must be addressed: The defining and classifying of social media types to relevantly regulate them:**
>
> There should be 2 categories of social media apps: the communication- the communication-focused social media and the Sharing-Focused Social Media. They should be in different categories given that they play very different roles. Sharing-Focused social media is the source of problems that motivated the act: such as cyberbullying, gory/violent content, pornography, content that encourages self harm

or violence, and algorithmic influence (which leads to extremism, misinformation, disinformation and echo-chambers). While the Communication-Focused social media is the source of the main defences of social media such as social connectivity, communication, and a lack of unsolicited harmful content. This is why it makes sense to limit access to the Sharing-focused Social media and promote the Communication-Focused Social media. Through this, the ban can be more “Swiss army-like” and less “like a machete” in the words of Mr. French. This will satisfy much of the opposition to this ban in the process, while also satisfying the parents who are concerned about their children.

A robust definition of the Communication-focused Social Media could be: "Communication-focused social media refers to online platforms, applications, or services that primarily facilitate direct, real-time, or asynchronous communication between users. These platforms are designed to enable private or semi-private exchanges of text, voice, video, or other forms of communication, typically within closed or controlled groups and networks. The primary purpose of these platforms is to foster interpersonal communication rather than the public dissemination of content.” Examples include apps like WhatsApp, Discord, Signal, and Telegram

A robust definition of Sharing-Focused Social Media could be “Sharing-focused social media refers to online platforms, applications, or services primarily designed for the public or semi-public dissemination of user-generated content. These platforms facilitate the sharing of multimedia content such as photos, videos, texts, and other creative works to a broad or public audience. The primary purpose of these platforms is to enable users to publish content that can be viewed, interacted with, or redistributed by others, often outside the original creator's control." Examples include apps like Instagram, Facebook, TikTok, and Twitter.

Key Features of Communication-focused social media:

- Primary Function: The central function of these platforms is to enable direct and often private communication between individuals or groups. Content shared is typically intended for a specific audience and not the general public.
- Privacy and Control: Users generally have higher control over who can access their communications. Group sizes can vary but are often restricted by platform design.
- Content Permanence: The communication may be transient, with options for messages to disappear after a certain period or be deleted by the users.
- Engagement: Engagement is typically in the form of direct responses (e.g., replies, reactions) within the communication thread.

Key Features of Sharing-focused Social Media:

- Primary Function: The main function is to share content with a broader audience, with features designed to maximise visibility and engagement (e.g., likes, shares, comments).
- Audience Reach: Content is typically designed to reach a wider, often public audience. Even when privacy settings are applied, the default or encouraged behaviour is toward public or semi-public sharing.

- Content Permanence: Content often has a more permanent presence, being archived and accessible unless deliberately removed. Even then, content might be reshared or saved by other users.

- Engagement: Engagement involves public interactions such as comments, likes, shares, and other forms of community feedback, often visible to other users.

Key Differences:

- User Intent and Interaction: Communication-focused platforms are built around personal and controlled interactions, while sharing-focused platforms are centred on content dissemination and public engagement.

- Audience Control: Communication platforms offer granular control over who participates in the conversation, while sharing platforms often encourage or enable broader content visibility.

- Content Nature: In communication platforms, the content is typically conversational and intended for immediate, direct engagement. In sharing platforms, the content is more often curated and designed for broader, often public, consumption and interaction.

[A 13 Year old]

Youtube kids is really, REALLY cursed, Like honestly, normal youtube is better than youtube kids, It's moderation recognizes anything colourful and bright as kid content, inappropriate minecraft animations, s*x, and other things are on there- while yes, it does come with some restrictions, it also limits what people know, for school you look at youtube for homework things, and youtube kids doesn't have any helpful school sources for 10-14 year olds- it's all just "I survived 100 days in minecraft hardcore mode". And nothing on youtube kids is fun to watch for 10-14 year olds- 14-13 year olds watching brain rot is a very, very bad idea. (sic)

But the things on youtube are not good either, even more things get past on youtube. But you can't really stop kids from going on to these websites, and everyone just ignores them, the thing that would make it safer online is things like showing information to parents, going through schools, not lecturing the kids- they will just ignore it- but lecture the parents, they are the ones who will enforce it- Most parents don't know what the kids are watching, or don't understand the significance.[160] (sic)

Comment

The additional submissions received from the eSafety Youth Council were well formulated and reflect the importance of hearing the voices of young people who might be affected in one way or another by the proposed restrictions. The distinction between communication-focused and sharing-focused social media is important and would perhaps be relevant to determining what

[160] eSafety Youth Council, Additional submissions to the Honourable Roert French AC, received 29 August 2024.

social media services could be treated as exempt social media services under the proposed legislation.

Chapter 13 — The legislative powers of the State of South Australia[161]

It is essential that any law put to the South Australian Parliament to provide for access restrictions to social media be within the law-making powers of that Parliament.

Those powers are found in the *Constitution Act 1934* (SA) and the *Australia Acts 1986*. Section 5 of the *Constitution Act* provides:

> The Legislative Council and House of Assembly shall have and exercise all the powers and functions formerly exercised by the Legislative Council constituted pursuant to section 7 of the Act of the Imperial Parliament, 13 and 14 Victoria, Chapter 59, entitled "An Act for the better Government of Her Majesty's Australia Colonies.

The reference to 13 and 14 Vict c 59, is a reference to the *Australian Constitutions Act 1850*. Section 7 of that Act provided for the establishment of a Legislative Council in South Australia. Section XIV of that Act conferred upon the Legislative Council of South Australia (along with the colonies of Victoria, Van Diemen's Land and Western Australia):

> … to make Laws for the Peace, Welfare, and good Government of the said colonies respectively …

The Australia Act 1986 (UK) and the *Australia Act 1986* (Cth) were enacted as part of the final severance of the constitutional authority of the United Kingdom Parliament over the Australian States. They both provide in s 2:

> **2 Legislative Powers of Parliaments of States**
>
> (1) It is hereby declared and enacted that the legislative powers of the Parliament of each State include full power to make laws for the peace, order and good government of that State that have extra-territorial operation.
>
> (2) It is hereby further declared and enacted that the legislative powers of the Parliament of each State include all legislative powers that the Parliament of the United Kingdom might have exercised before the commencement of this Act for the peace, order and good government of that State but nothing in this subsection confers on a State any capacity that the State did not have immediately before the commencement of this Act to engage in relations with countries outside Australia.

[161] I am grateful for the helpful review of this Chapter by Professor John Williams and Emeritus Professor Geoffrey Lindell of the University of Adelaide. Errors and omissions remain mine alone.

The proposed legislation would impose duties on the providers of social media services, many of whom may be located in other countries. Although s 2(1) of the *Australia Act* itself provides that the States may legislate extra-territorially, the words 'peace order and good government' suggest that legislation enacted by a State must have some nexus with it. In his text on the South Australian Constitution, the late Brad Selway, a former Solicitor-General of South Australia and later a Judge of the Federal Court of Australia wrote:

> There must be some connection between the State and the extra-territorial persons, things or events on which the law operates although a remote and general connection will suffice.[162]

This view has been supported in commentary upon s 2(1) of the *Australia Acts 1986*. Professor Anne Twomey in a text published in 2004 on the Constitution of New South Wales observed:

> The negotiations leading up to the enactment of the Australia Acts show that the aim of the States in pursuing the insertion of such a provision [i.e. extra-territorial legislative power] was to ensure that any limitations on their legislative power derived from their 'subordinate' or 'colonial' status were removed. It was recognised that a nexus requirement would remain, as this was necessary to support the federal system. It was therefore agreed that the reference to the 'peace order and good government' of the States should be expressly included in the provisions. Further, and most significantly, s 5 of the Australia Acts provides that s 2 is subject to the Commonwealth Constitution. Thus, to the extent that an extra-territorial limitation upon State legislative power is derived from the federal structure imposed by the Commonwealth Constitution, s 2(1) does not remove that limitation.

In *Union Steamship Co of Australia v King* the High Court linked the need for a territorial connection to the position of the States within a federation, stating:

> And as each State Parliament in the Australian Federation has power to enact laws for its State, it is appropriate to maintain the need for some territorial limitation in conformity with the terms of the grant, notwithstanding the recent recognition in the constitutional rearrangements for Australia made in 1986 that State Parliaments have power to enact laws having an extra-territorial operation: see Australia Act 1986 (Cth), s 2(1); Australia Act 1986 (UK) s 2(1).[163]

The character of that passage as a recognition of territorial limitations upon the legislative powers of the States arising from the federal structure of which each State is a part, was affirmed in *State Authorities Superannuation Board v Commissioner of Taxation (WA)*.[164]

---

162 Brad Selway, *The Constitution of South Australia* (Federation Press, 1997) 65 citing *Port MacDonnell Professional Fishermen's Association Inc v South Australia* (1989) 168 CLR 340, 372 and *Union Steamship v King* (1988) 166 CLR 1, 10 and 14; *State Authorities Superannuation Board v Commissioner of State Taxation (WA)* (1996) 189 CLR 253.

163 *Union Steamship Co of Australia v King* (1988) 166 CLR 1, 14.

164 (1996) 189 CLR 253, 271 (Brennan CJ, Dawson, Toohey and Gaudron JJ).

The nature of the necessary connection of legislation to the State is broad. In *Broken Hill South Ltd v Commissioner of Taxation (NSW)*[165] Dixon J said:

> It is within the competence of the State legislature to make any fact, circumstance, occurrence or thing in or connected with the territory the occasion of the imposition upon any person concerned therein of a liability to taxation or other liability …. It is also within the competence of the legislature to base the imposition of the liability on no more than the relation of the thing to the territory. The relation may consist in presence within the territory, residence, domicile or carrying on business there, or even remoter connections. If a connection exists it is for the legislature to decide how far it should go in the exercise of its power.[166]

Brad Selway in his text offered a qualification on the breadth of the linkage condition:

> It may be that the State's extra-territorial legislative power is limited even where there would appear to be a relevant nexus to South Australia, because the subject matter falls within the legislative power of another government. Such subject matters would include real property situated in another State, or the duties of officers of the other government and would include the law to be applied by the courts of another jurisdiction.[167]

He also suggested that there may be a limitation on the legislative power of the State to legislate inconsistently with the laws of another State which has a greater nexus to the subject matter.[168]

None of these limitations would constrain the State Parliament of South Australia from legislating to regulate, by laws of general application, the conduct within South Australia of a corporation, foreign or Australian, or a person resident in another country, State or Territory. The provision of social media services to persons living within South Australia is conduct within or connected to the State, sufficient to meet the nexus requirement where the provider is a foreign corporation or resident of another State or country. That said, the link to South Australia should be made explicit in the legislation.

A State law co-existing with a Commonwealth law on the same subject matter

The examination has had regard to the existing regulatory framework under Commonwealth law — specifically the *Online Safety Act*. It is important that any South Australian law not be

---

165 (1936) 56 CLR 337.

166 Ibid 375.

167 Selway, above n 162, 5.2.7.1.

168 Selway, above n 162, 5.2.7.2. There is an unresolved question of how to resolve inconsistency between overlapping State and State and Territory laws. One approach — a choice of law approach considers which jurisdiction has the closest connection with the law. The other involves an approach analogous to s 109 of the *Constitution* with primacy given to the State in which the matter regulated takes place — see generally Geoffrey Lindell and Sir Anthony Mason. 'The Resolution of Inconsistent State and Territory Legislation' (2010) 38 *Federal Law Review* 391.

inconsistent with applicable Commonwealth law. Section 109 of the *Constitution* would render an inconsistent State law invalid to the extent of any inconsistency. That said, it is constitutionally open to South Australia to adopt a more restrictive content neutral regulatory measure in relation to children than presently applies at Commonwealth level. The Commonwealth legislation allows for that possibility in s 234, which provides:

> It is the intention of the Parliament that this Act is not to apply to the exclusion of a law of a State or Territory to the extent to which that law is capable of operating concurrently with this Act.

Such a provision cannot overcome invalidity flowing from direct inconsistency between a Commonwealth law and a State law. It does, however, negative the proposition that the Commonwealth law is intended to cover the field of the operation to the exclusion of any State law.[169] The prescription or adoption of special standards covering online safety in regard to children as is provided in s 138(2)(f), (s) (t), (zh), (zi), (zj) in the *Online Safety Act* is unlikely to be read as creating a right or permission to provide online services to children so as to give rise to direct inconsistency. The standards in question are more likely to be regarded as standards to be observed *if and as long as* those services can be lawfully provided by State law having regard to the clearly evinced intention of the Commonwealth Parliament in the same Act not to cover the field.

There would not seem to be any risk of infringement of any constitutional guarantees or immunities under s 92 or s 117 of the *Constitution*.[170] The latter provision states that:

> A subject of the Queen, resident in any State, shall not be subject in any other State to any disability or discrimination which would not be equally applicable to him if he were a subject of the Queen resident in such other State.

A proposed law, applicable to providers located, delivering or allowing access to social media services in South Australia does not discriminate in South Australia against the residents of other States. The access restriction proposed would restrict access to children living in South Australia and not to those from other States or outside Australia, holidaying or visiting South Australia. There is a question about the appropriate legal term to be used in any statute to define the application of the restriction. The term 'domicile' may be appropriate in this context. Thus a child domiciled in South Australia is a child for whom South Australia is their permanent

---

169 *R v Credit Tribunal*; *Ex parte General Motors Acceptance Corporation* (1977) 137 CLR 545, [564].

170 Or the statutory equivalents of the guarantee of the freedom of trade commerce or intercourse between the States and the ACT and the NT contained in the Commonwealth laws which are their self-government Acts.

home or who lives in and has a substantial connection with South Australia. Such a child does not cease to be domiciled in South Australia simply because he or she travels to another State or overseas.

The implied freedom of political communication would not seem to be engaged. The restriction is content neutral, is not directed at political speech and, in any event, is a reasonable and proportionate means for a legitimate purpose consistent with Australia's representative democracy.

The Regulator — legislative options

Any Act imposing age-related restrictions upon access to social media in South Australia will need to have someone to administer and enforce it. That is to say, there will have to be a regulator.

It is obviously open to South Australia to create its own bespoke regulator or to confer additional functions on an existing statutory officer such as the Children's Commissioner or the Commissioner for Consumer Affairs. However, the timeline and resources necessary to get a State Regulator, whether new or existing, fully functional and operating could be significant. As appears from the issues canvassed in this Report, the regulatory landscape is complex, even allowing for a narrow cast access restriction which does not involve regulation of content. Any regulator would necessarily have to be supported by officers with the expertise and experience necessary to administer and enforce the legislation. As appears from the model proposed, the regulator would be closely involved in developing criteria for exempt social media to which any restriction would not apply, and for providing regulatory guidance as to reasonable steps which a provider would be expected to take to comply with the restrictions imposed by the legislation. There would inevitably be some duplication of resources with those provided to the Commonwealth regulator.

An alternative approach would be to secure the agreement of the Commonwealth to confer a new State-based regulatory function upon the Commonwealth eSafety Commissioner. There is precedent for that approach in national regulatory schemes. Examples are:

Section 13A — *Australian Energy Market Act 2004*

Section 6AAA — *Therapeutic Goods Act 1989*

It the State law does not impose any 'duty' on the Commonwealth regulator the consent of the Commonwealth Parliament set out in a law of the Commonwealth would suffice. If the State law purports to confer a duty upon the Commonwealth regulator, that must be a duty which falls within a Commonwealth head of power and is supported by a law of the Commonwealth.

In *R v Hughes* six Justices of the High Court stated:

> It may be accepted that, subject to what may be the operation of negative implications arising from the *Constitution*, for example Ch III, in the exercise of the incidental power the Parliament may permit officers of the Commonwealth holding appointments by or under statute to perform functions and accept appointments in addition to their Commonwealth appointments. [171]

The Justices added two further propositions:

> The first is that a State by its laws cannot unilaterally invest functions under that law in officers of the Commonwealth; the second is that a State law which purported to grant a wider power or authority than that the acceptance of which was prescribed by Commonwealth law would, to that extent, be inconsistent with the Commonwealth law and invalid under s 109 of the Constitution.[172]

In relation to the imposition by federal law upon Commonwealth officers of duties to perform functions or exercise powers created and conferred by State law, the Justices said '[s]uch a federal law must be supported by a head of power.'[173]

It was also said in *Hughes* to be 'beyond question' that the executive power of the Commonwealth extends to entry into governmental agreements between the Commonwealth and the States on matters of joint interest, including matters which require for their implementation joint legislative action, so long as the end to be achieved and the means by which it is to be achieved are consistent with and do not contravene the *Constitution*.[174]

Further, the incidental power, s 51(xxxix) of the *Constitution* authorises the Parliament to make laws in aid of an exercise of the executive power. However the Court cautioned that that proposition 'remains open to some debate'. The *Hughes' case* was 'not a suitable occasion to continue it.'[175]

---

171 (2000) 202 CLR 535, [31].
172 Ibid.
173 Ibid [32].
174 Ibid 555, [38].
175 Ibid 555, [39].

The problem is probably illusory in that an age-based restriction upon access to social media services is well within the legislative powers of the Commonwealth. In the exercise of those powers it is reasonably arguable that it could directly confer upon the Commonwealth Regulator the power to exercise functions, the content of which would be defined by the State law at the time of the enactment of the Commonwealth law.

All that being said, it remains the case that efficient use of resources and the avoidance of undue complication in the administration of age restricted access would be better served by a national scheme rather than a patchwork of State-based restrictions which necessarily must be qualified by reference to territorial links with the State and bring in concepts of domicile or residency to describe the classes of children to which the restrictions would apply.

This Examination does not consider in detail the issues raised in relation to the enforcement of remedies against foreign corporations which are providers of social media services in Australia. It is reasonably arguable that such providers are carrying on business in Australia. If foreign corporations, they are required to be registered in Australia with a local agent and a registered office upon which documents can be served. Those requirements are imposed under the *Corporations Act 2021*(Cth).[176] For proceedings which may involve service of documents out of the jurisdiction, Schedule 1 to the Uniform Civil Rules 2020 (SA) provides for service overseas. Section 2 of that Schedule allows for originating process to be served out of Australia without leave in a case in which the claim concerns the construction, effect or enforcement of an Australian statute.

Section 8 provides that documents other than an originating process may be served outside Australia with the lease of the Court. The Schedule also provides for service under the Hague jurisdiction in civil or criminal matters.

Questions of the enforcement of injunctions, compensation orders, civil damages awards and civil penalties against a foreign corporation raise a variety of legal issues, which face every Australian regulator whether national or State dealing with foreign corporations. There have been some apposite examples of regulatory action. One such was *Valve Corporation v Australian Competition and Consumer Commission*.[177] Valve Corporation's website, which was a US website not an Australian website, contained representations to consumers which

176 Corporations Act, s 601, s 601(CF) and s 602(CX).
177 (2017) 258 FCR 190.

allegedly misrepresented their legal rights. The Federal Court held that the representations constituted engaging in conduct in Australia for the purposes of the Australian Consumer Law.

In 2020, the Australian Information Commissioner commenced proceedings in the Federal Court against Facebook Inc and Facebook Ireland Ltd alleging contravention of provisions of the *Privacy Act* with respect to 311,127 Australian Facebook users between 12 March 2014 and 1 May 2015. The Commissioner sought declarations and civil pecuniary penalties under the Act. The proceedings were contested at the outset on the basis that the Federal Court lacked jurisdiction to decide the dispute. The companies against which the Commissioner proceeded were not located in Australia. Facebook Inc (Meta) was incorporated in Delaware and headquartered in California. Facebook Ireland was a Meta subsidiary based in Ireland. Neither was registered to carry on business in Australia. Facebook Inc's subsidiary, Facebook Australia Pty Ltd was not party to the proceeding.

The Commissioner applied ex parte to serve the respondents out of the jurisdiction and orders were made on 22 April 2020. Facebook Inc then applied to set them aside.

The relevant provisions of the *Privacy Act* applied to 'an act done or practice engaged in or outside Australia' by an entity with an 'Australian link'. An entity would have an Australian link if it carried on business in Australia. Facebook Inc argued that the Commissioner had failed to establish that Facebook carried on business in Australia. That argument was rejected at first instance. The Full Court of the Federal Court of Australia dismissed the appeal against the first instance decision.[178] Part of the business conducted by Facebook Inc was the installation of cookies on Australian users' devices and the provision to Australian developers of a platform by which developers could enable third party applications to utilise the Facebook login. The Full Court found there was a prima facie case that Facebook Inc was carrying on business in both foreign jurisdiction and in Australia which was sufficient to engage the relevant provision of the *Privacy Act*.

On 7 March 2023, a Full Bench of the High Court revoked a grant of special leave which had been made. It did so on application by the Commissioner on the basis that the Rules relating to the requirements of service had changed and that the grounds of appeal were no longer of public importance.

178 *Facebook Inc v Australian Information Commissioner* (2022) 289 FCR 217.

Questions of offshore enforcement in relation to the exercise of investigative powers and remedies awarded by the Supreme Court of South Australia, may involve more than one mode of engagement with foreign jurisdictions. These are issues with which all regulators of social media services around the world have to grapple. South Australia will be no exception. The question, however, is not one which goes to the power of the South Australian legislature, but rather the mechanisms available to a Regulator in the enforcement of the Act.

Chapter 14: A Draft Bill

The features of a legislative model for South Australia to give effect to age-based restrictions on access to social media services have already been set out in Chapter 1. What follows in this Chapter is a draft Bill for a law which might give effect to the Government's policy.

The Bill proposes a law which applies to social media services, the definition of which is based upon the definition in the *Online Safety Act* of the Commonwealth. It is not identical to that definition. The Bill provides for exempt social media services which do not pose a risk to the safety of children. It imposes two duties of care on social media service providers. The first is not to allow access to a non-exempt social media service by children under the age of 14 nor by children aged 14 or 15 without their parents' consent.

The Bill provides for a 'reasonable steps' criterion for compliance with that duty. The second duty of care is to positively take reasonable steps to prevent such access in the relevant age ranges. The Bill provides for a Regulator to enforce the law and arms the Regulator with functions and powers for that purpose.

There is a range of enforcement mechanisms for breach of the duties, including infringement notices, compensation orders and declarations, injunctions, civil damages and civil penalties for wilful, reckless or repeated breaches. It would also be open to the Government to include provision for non-punitive remedial notices and enforceable undertakings. These have not been included in the Draft Bill as they attract a number of ancillary provisions.

The Regulator's role includes the development of guidance for what might constitute reasonable steps necessary to comply with the duties imposed by the law. The Regulator will also be able to develop criteria for determining which social media services should be exempt from the application of the Act. There is also provision for a pro-active research and policy development role.

It is to be emphasised that the Bill is an indicative model. It is not proposed as a definitive statement of what the law should be. At the very least it should offer some guidance as to an approach which can be taken in South Australia in formulating a law to give effect to the Government's policy.

The Bill does not offer the only possible legislative mechanism for giving effect to the South Australian Government's policy. As appears from the earlier Chapters of this Report, the concept of 'social media' is dynamic and evolving. The framing of the definition of 'social media services' is challenging. The preferred option is for a broad generic definition, based on the definition in the *Online Safety Act* and coupled with a regulatory process for determining exempt social media services. There are, however, a number of options in the definition which may be considered. They are not exhaustive and are intended to be, so far as possible, compatible with existing Commonwealth law. Each option provides for exempt social media services to be prescribed by regulation or ministerial notice.

Option 1: The definition of 'social media service' as contained in the *Online Safety Act* (without amendment):

> **… *social media service*** means:
>
> (a) an electronic service that satisfies 1 or more of the following conditions:
>
> (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;
>
> (ii) the service allows users to link to or interact, or interact with, some or all of the other users;
>
> (iii) the service allows users to post material on the service;
>
> (iv) the service satisfied any other conditions prescribed by the regulations; or
>
> (b) a service, or service of a class, prescribed by the regulations;
>
> but does not include an exempt social media service.
>
> (2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

This definition achieves the greatest consistency with the current Commonwealth definition. However it does not account for the increasing convergence of 'communication focused services' and 'sharing focused services'.

This definition could also capture 'internet search engines' and 'app distribution services' as defined in the *Online Safety Act*. Whether these services could be determined to be exempt services would depend upon whether they were considered to be child safe and beneficial by the South Australian Government.

This definition could include Facebook, Instagram, TikTok, Snapchat, Pinterest and YouTube.

Option 2: The definition of 'social media service' as contained in the *Online Safety Act* and <u>including</u> messaging services/online gaming:

> ***social media service*** means—
>
> (a) an electronic service that satisfies 1 or more of the following conditions:
>
> (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;
>
> (ii) the service allows users to link to or interact, or interact with, some or all of the other users;
>
> (iii) the service allows users to post material on the service;
>
> (iv) <u>the service is a relevant electronic service;</u>
>
> (v) the service satisfied any other conditions prescribed by the regulations; or
>
> (b) a service, or service of a class, prescribed by the regulations;
>
> but does not include an exempt social media service;
>
> (2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

This definition would account for the increasing convergence between communication focused messaging services and social media services. The definition of 'relevant electronic services' as contained in s13A of the *Online Safety Act*, however, is broad and captures electronic services with a broad range of characteristics and potential risk profiles to children, including:

(i) a service that enables end-users to communicate, by means of email, with other end-users;

(ii) an instant messaging service that enables end-users to communicate with other end-users;

(iii) an SMS service that enables end-users to communicate with other end-users;

(iv) an MMS service that enables end-users to communicate with other end-users;

(v) a chat service that enables end-users to communicate with other end-users;

(vi) a service that enables end-users to play online games with other end-users;

Services within this category may be considered to have a lower risk profile for children (such as SMS services) and services used in the educational settings (such as email) and could be eligible for determination as 'exempt social media services'.

This definition could still capture internet search engine services and app distribution services as defined in the *Online Safety Act.*

For example this definition could include the platforms described in Option 1 and other services such as WhatsApp, Discord, Telegram, Roblox and Fortnite.

Option 3: The definition of 'social media service' as contained in the *Online Safety Act* including messaging services and online gaming and excluding internet search engine services and app distribution services.

> ***social media service*** means—
>
> (a) an electronic service that satisfies 1 or more of the following conditions:
>
> (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;
>
> (ii) the service allows users to link to or interact, or interact with, some or all of the other users;
>
> (iii) the service allows users to post material on the service;
>
> (iv) the service is a relevant electronic service;

(v) the service satisfied any other conditions prescribed by the regulations; or

(b) a service, or service of a class, prescribed by the regulations;

but does not include:

(c) a service that is an internet search engine service; or

(d) a service that is an app distribution service; or

(e) an exempt social media service;

(2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

This definition could potentially reduce the administrative burden of prescribing services captured by the definition which would ordinarily be considered to be of low risk to children and critical to their broader engagement in beneficial uses of online technology. If the definitions canvassed at Options 1 and 2 were applied, these classes of services could be eligible for determination as exempt services even though not expressly excluded in those Options.

For example, this definition could exclude the platforms described in Options 1 and 2 and exclude services such as Google, Bing, Yahoo, Google Play and the Apple App Store.

Option 4: The definition of 'social media service' as contained in the *Online Safety Act*, excluding messaging services, online gaming, internet search engine services and app distribution services

social media service means—

(a) an electronic service that satisfies 1 or more of the following conditions:

(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;

(ii) the service allows users to link to or interact, or interact with, some or all of the other users;

~~(iii) relevant electronic service;~~

(iii) the service allows users to post material on the service;

(iv) the service satisfied any other conditions prescribed by the regulations; or

(b) a service, or service of a class, prescribed by the regulations;

but does not include:

(c) a relevant electronic service; or

(d) a service that is an internet search engine service; or

(e) a service that is an app distribution service; or

(f) an exempt social media service;

(2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

If it is determined by the South Australian Government that the risks and harms posed by communication focused messaging and online gaming services were acceptable, the definition could exclude 'relevant electronic services' from its scope. However, given the convergence described above, it could prove challenging to distinguish messaging and online gaming services from the social media services captured by the definition.

This definition would include the services set out in Option 1 and exclude services such as those set out in Options 2 and 3.

Option 5: The definition of 'social media service' as contained in the *Online Safety Act,* excluding internet search engine services and app distribution services and silent on messaging services and online gaming

social media service means—

(a) an electronic service that satisfies 1 or more of the following conditions:

(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;

(ii) the service allows users to link to or interact, or interact with, some or all of the other users;

~~(iii) relevant electronic service;~~

(iii) the service allows users to post material on the service;

(iv) the service satisfied any other conditions prescribed by the regulations; or

(b) a service, or service of a class, prescribed by the regulations;

but does not include:

~~(c) a relevant electronic service; or~~

(c) a service that is an internet search engine service; or

(d) a service that is an app distribution service; or

(e) an exempt social media service;

(2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

The definition of 'social media service' in the Draft Bill is in line with Option 2. The choice of option is ultimately a matter for Government and the Parliament.

The choices presented by the Options reflect legislative models which may differ in the extent to which they expressly exclude certain services in the definition of 'social media service' on the one hand or, on the other, adopt a very broad definition leaving it to the exemption process to determine which services are excluded.

South Australia

Children (Social Media Safety) Bill 2024

A BILL FOR

An Act to protect children from harm by restricting access to social media.

Contents

The Parliament of South Australia enacts as follows:

1—Short title

This Act may be cited as the *Children (Social Media Safety) Act 2024*.

2—Act to bind

This Act comes into operation on a day to be fixed by proclamation.

3—Interpretation

(1) In this Act—

….

access to a social media service incudes any use of such a service but does not include access that is only for the purposes of establishing the age of the person or whether the person has parental consent to access the service;

child means a person under the age of 16 years;

compensation order means an order under section 11;

duty of care under this Act–see section 8;

electronic service means –

(a) a service that allows end-users to access material using a carriage service; or

(b) a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service;

but does not include:

(c) a broadcasting service; or

(d) a datacasting service (within the meaning of the *Broadcasting Services Act 1992*);

exempt social media service means any social media service which is designated by a notice published by the Minister as an exempt social media service or which is a member of a class of social media services so designated by the Minister;

Fund means the *Children's Online Safety Fund* established under section 13;

online social interaction includes online interaction that enables users to share material for social purposes;

parent, of a child or young person, includes—

(a) a step-parent; and

(b) a person who stands in *loco parentis* to the child or young person;

provider of a social media service is a person who makes the service available for use by persons in South Australia and includes persons who participate in the provision of the service in South Australia;

Regulator means the Regulator appointed under this Act;

relevant electronic service means

(a) any of the following electronic services:

(i) a service that enables end-users to communicate, by means of email, with other end-users;

(ii) an instant messaging service that enables end-users to communicate with other end-users;

(iii) an SMS service that enables end-users to communicate with other end-users;

(iv) an MMS service that enables end-users to communicate with other end-users;

(v) a chat service that enables end-users to communicate with other end-users;

(vi) a service that enables end-users to play online games with other end-users;

(vii) a service, or service of a class, prescribed by the regulations;

social media service means—

(a) an electronic service that satisfies 1 or more of the following conditions:

(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more users;

(ii) the service allows users to link to or interact, or interact with, some or all of the other users;

(iii) the service allows users to post material on the service;

(iv) the service is a relevant electronic service;

(v) the service satisfied any other conditions prescribed by the regulations; or

(b) a service, or service of a class, prescribed by the regulations;

but does not include an exempt social media service;

(2) In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of ***social media service*** in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.

4—The application of the Act

(1) This Act applies to any person wherever located who provides or offers to provide or allows access to a social media service to end users within this State.

(2) The duties of care imposed on social media service providers by this Act apply with respect to children domiciled within this State or who have resided in the State for a continuous period of more than three (3) months.

Note: The Act is not intended to apply to children visiting South Australia on a temporary basis.

5—Objects and principles

(1) The objects of this Act are to prevent or mitigate the risk of psychological and other harms to children flowing from unrestricted access to social media platforms and services.

(2) The paramount consideration in the administration, operation and enforcement of this Act must be to ensure that children are protected from the risk of harm.

6—The Regulator of Child Social Media Safety

(1) There will be a Regulator of Child Social Media Safety.

(2) The Regulator will be appointed by the Governor on the recommendation of the Minister and is an agency of the Crown.

(3) The person appointed as Regulator—

(a) should have a detailed understanding of social media services and the issues affecting child social media safety;

(b) may be a public service employee.

7—Powers of the Regulator

The Regulator has power to do all things necessary or convenient to be done for or in connection with the performance of the Regulator's functions.

Drafting Note: *The final bill would include administrative provisions such as the terms and conditions the Regulator's appointment and its functions.*

….

8—Duties of care on providers of social media services.

(1) A provider of a social media service which is not an exempt social media service has a duty of care to prevent access to that service in this State by:

(i) any child domiciled in the State who is under the age of 14 years; and

(ii) any child domiciled in the State who is aged 14 or 15 years unless the provider has been notified that a parent of the child consents to the child's access to the service.

(2) A provider of social media has a duty of care to take all reasonable steps to prevent access to that service in this State by:

(i) any child domiciled in the State who is under the age of 14 years; and

(ii) any child domiciled in the State who is aged 14 or 15 years unless the provider has been notified that a parent of the child consents to the child's access to the service.

9—Complaints about a breach of the duty of care

If a person has reason to believe that a child domiciled in this State has been or is being provided with access to a social media service which is not an exempt social media service contrary to the duty of care imposed by section 8(1), then the person may, on behalf of the child, make a complaint to the Regulator about the breach.

…

10— Infringement Notice

(1) If the Regulator believes on reasonable grounds that a provider of a social media service has contravened a duty of care under section 8, the Regulator may give to the person an infringement notice for the alleged contravention.

(2) The infringement notice must state the amount that is payable under the notice.

(3) The amount stated in the notice for the purposes of paragraph (2) shall be prescribed in the Regulations.

(4) Where the amount specified in the infringement notice is paid, it shall be paid into the Fund, established under section 13.

Drafting Note: *The final bill would include provisions in relation to the Regulator's powers.*

….

11—Enforcement of duties of care

(1) If, on application by the Regulator, the Supreme Court is satisfied, on the balance of probabilities, that a provider of social media has breached a duty of care under this Act, the Court may—

(a) make a declaration to that effect; and

(b) order the payment of compensation by the provider in accordance with the prescribed scale; and

(c) in the event that the Court is satisfied that the breach of duty was wilful or reckless, or was a repeated breach, impose a civil penalty;

(d) make any ancillary orders the Court thinks fit including an injunction.

(2) The regulations may prescribe a scale of compensation amounts for the purposes of this section, with such amounts increasing according to the scope and seriousness of any breach of the duty of care under this Act.

(3) All compensation ordered to be paid under this section is payable to the Fund in accordance with section 13.

(4) The Regulations may prescribe civil penalties which may be imposed by the Supreme Court in the case of wilful or reckless or repeated breaches of the duties imposed by this Act.

Drafting Note: *The final bill could include additional provisions for the Regulator to issue remedial notices and to agree upon enforceable undertakings.*

(5) A breach of the duty of care under section 8(1) of this Act in relation to a social media service is established, for the purposes of this section, by evidence that a person has been able to access the social media service in this State without being required to establish that the person—

(a) is not a child under the age of 14 years; and

(b) is not a child aged 14 or 15 years who is accessing the service without the consent of a parent.

(6) It is a defence to an action by the Regulator for a breach of the duty of care under section 8(1) of this Act if the provider of the social media service proves that, at the time of the breach, the provider had taken all reasonable steps to prevent access to its social media service.

(7) A breach of the duty of care imposed by subsection 8(2) of the Act occurs where the provider of a social media service fails to take or maintain reasonable steps to provide access to that service in South Australia as required by subsection 8(2).

(8) The regulations may prescribe measures that will, or will not, be taken to constitute reasonable steps for the purposes of establishing the defence under subsection (6) and for the purposes of complying with the duty under subsection 8(2).

12—Damages

(1) If—

(a) a provider of social media breaches the duty under this Act; and

(b) a child to whom the duty of care under this Act applies—

(i) has access to the social media service contrary to the provisions of section 8; and

(ii) suffers mental or physical harm as a result of that access,

the breach of duty of care is actionable as a tort by the child (and damages may be awarded against the provider as if the breach of duty of care constituted negligence by the provider).

(2) An action may be brought under this section on behalf of the child by—

(a) a parent of the child; or

(b) the Regulator (in the Regulator's absolute discretion).

13—Children's Online Safety Fund

(1) The *Children's Online Safety Fund* is established.

(2) The Fund will consist of—

(a) any compensation amounts paid under this Act; and

(b) any amounts paid pursuant to an infringement notice under this Act; and

(c) income and accretions from investment of money from the Fund; and

(d) any money appropriated by Parliament for the purposes of the Fund.

(3) Any money in the Fund that is not for the time being required for the purposes of the Fund may be invested by the Regulator in any manner approved by the Minister.

(4) The Regulator may apply any portion of the Fund towards—

(a) paying any costs or expenses incurred in the administration or enforcement of this Act (including any costs and expenses incurred in relation to the identification of social media services that should be exempt social media services under this Act); and

(b) research into the provision of safe and beneficial social media services for children; and

(c) discretionary payments for the benefit of children who have, in the opinion of the Regulator, suffered mental or physical harm as a result of a breach of the duty of care under this Act; and

(d) education programs relating to social media safety for children; and

(e) any other prescribed purposes.

(5) The Regulator must keep proper accounts of receipts and payments in relation to the Fund.

(6) The Auditor-General may at any time, and must at least once in each year, audit the accounts of the Fund.

14—Regulations

(1) The Governor may make such regulations as are contemplated by, or necessary or expedient for the purposes of, this Act.