Reset·Tech
AUSTRALIA

Response to the Senate Legal & Constitutional Affairs Legislation Committee inquiry into the Privacy and Other Legislation Amendment Bill 2024

Reset.Tech Australia
Oct 2024

Summary

Australia's privacy laws are substantially out-of-date and ineffective in the digital age. We welcome the renewed focus on updating and improving our regulatory framework. Noting that many of the necessary and positive proposals put forward in the *Privacy Act Review Report*[1] have been 'postponed' for a further tranche of reforms, we nonetheless welcome the initial steps outlined in the Privacy and Other Legislation Amendment Bill 2024. In particular, we warmly welcome:

- The introduction of a Children's Privacy Code, and
- The proposals for additional powers for the OAIC to directly draft Codes where necessary, moving away from a default reliance on industry-drafted, co-regulatory models.

This short submission focusses on these two proposals, reinforcing their necessity, and outlining the need for further reforms in the near term.

[1]Office of the Attorney General 2023 *Privacy Act Review Report*
https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Contents

About Reset.Tech Australia & this submission

We welcome the opportunity to respond to the Senate Legal and Constitutional Affairs Legislation Committee's Inquiry into the Privacy and Other Legislation Amendment Bill 2024. Reset.Tech Australia is an Australian policy development and research organisation. We specialise in independent and original research into the social impacts of technology, including social media companies. We are the Australian affiliate of Reset.Tech, a global initiative working to counter digital harms and threats.

Australia's privacy laws are substantially out-of-date and ineffective in the digital age, and we welcome the renewed focus on updating and improving our regulatory framework. Noting that many of the necessary and positive proposals put forward in the *Privacy Act Review*[2] have been 'postponed' for a further tranche of reforms, we welcome the initial steps outlined in the Privacy and Other Legislation Amendment Bill 2024. In particular, we warmly welcome the introduction of a Children's Privacy Code, and the proposals for additional powers for the OIAC to move 'beyond' co-regulatory models for code development where necessary.

This short submission focusses on these two proposals, reinforcing their necessity, and outlining the need for further reforms in the near term.

Reset.Tech Australia has a dedicated, multi-year work program on privacy, with a special focus on children's privacy and collaborations across the children's sector. Our work on young people and privacy in Australia is generously supported by the Internet Society Foundation. Our reports include:

- *Best Interests and Targeting: Implementing the Privacy Act Review to advance children's rights*[3]
- *Prohibiting targeting to children and children's best interests: Can the two coexist?*[4]
- *Australians for Sale: Targeted Advertising, Data Brokering and Consumer Manipulation (section on children and young people)*[5]
- *Realising young people's rights in the digital environment*[6]
- *Capacity of the consent model online*[7]
- *How outdated approaches to regulation harm children and young people*[8]

We have also stood with sector colleagues for a number of years and campaigned for a Children's Online Privacy Code.[9]

[2]Office of the Attorney General 2023 *Privacy Act Review Report*
https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
[3]Reset.Tech Australia 2024 *Best Interests and Targeting*
https://au.reset.tech/news/best-interests-and-targeting-implementing-the-privacy-act-review-to-advance-children-s-rights/
[4] Reset.Tech Australia 2024 *Prohibiting targeting to children and children's best interests*
https://au.reset.tech/news/briefing-prohibiting-targeting-to-children-and-children-s-best-interests-can-the-two-coexist/
[5]Reset.Tech Australia 2023 *Australians for Sale* https://au.reset.tech/news/coming-soon-australians-for-sale-report/
[6]Reset.Tech Australia 2023 *Realising young people's rights in the digital environment*
https://au.reset.tech/news/report-realising-young-people-s-rights-in-the-digital-environment/
[7]Reset.Tech Australia 2023 *Capacity of the consent model online*
https://au.reset.tech/news/capacity-of-the-consent-model-online/
[8]Reset.Tech Australia 2022 *How outdated approaches to regulation harm children and young people*
https://au.reset.tech/news/capacity-of-the-consent-model-online/
[9]For more information, see Reset.Tech Australia 2024 *Children's Privacy Code*
https://www.childrensprivacycode.org.au/

1. Welcoming a Children's Privacy Code

We commend the proposals to introduce a Children's Privacy Code. Under Australia's current privacy regime, there are no special considerations or protections for children's data, despite the unique issues arising from this data. This creates serious risks given the huge amounts of data that is now collected about children; by the time a child turns 13, an estimated 72 million data points have been collected about them.[10] From before birth, where anxious parents upload data into pregnancy apps, to their first online learning app at primary school, to photos of their parties and gatherings shared on social media, almost every aspect of childhood now creates data that is inadequately protected under Australian law. By simply existing in a data-hungry society, Australian children generate a huge data footprint that can travel with them across their whole lives, and the move towards creating a Code that could govern data collection and use is both necessary and long overdue. Reset.Tech Australia, and a coalition of children's organisations, have been actively calling for a dedicated children's privacy code for a number of years.[11]

Data about children can create real risks; from risks of data leaks and identify theft and scams, to safety risks like the sale of kids' live location data. This data can obviously be harmful when it's handed to 'bad actors' like scammers and hackers. But even when it's in the hands of companies, like data brokers and ad techs, it can be used to harm. From the use of children's data to test and train addictive design features on social media apps, to education apps that track where kids are and share that data with advertisers, kids data isn't always used in ways that are in their best interests. A children's privacy code can help to put boundaries in place to protect children and their data.

Requirements around processing children's data in ways that are in their best interests would help prevent serious harms, such as to privacy, safety, and wellbeing. 'Best interests' is a long-standing child-rights principle that exists in other places in Australian law. In a digital and data context it would require that you can only collect, use, sell or share children's data in ways that are in their best interests. The widespread sharing and sale of kids' data, using it to target them with ads or addictive designs, or to create creepily detailed profiles about them for commercial purposes and other practices that cause serious harm could be limited through this approach.

We have some concerns about the capacity of Children's Privacy Code to effect broad and meaningful changes within the current Australian Privacy Principles and limitations of the current *Privacy Act* in general, especially given its proposed limited scope (restricted to social media, designated internet services and relevance electronic services, but excluding for example EdTech and data brokers). However, we believe that this is still desirable and a positive first step. We note there is much international precedent around this, with the UK, Ireland, California, France, Sweden and the Netherlands having comparable 'Codes' in place already that we may be able to learn from.[12]

While the impact and effectiveness of a Code will depend on the drafting process, **the instruction to the OAIC to develop a children's code is warmly welcomed and critical to the initiative's success.**

---

[10] Rebecca Stewart 2017 Adtech firms collecting 'vast amounts' of data on kids despite online regulations *The Drum* https://www.thedrum.com/news/2017/12/13/adtech-firms-collecting-vast-amounts-data-kids-despite-online-regulations

[11] For more information, see Reset.Tech Australia 2024 *Children's Privacy Code* https://www.childrensprivacycode.org.au/

[12] See for example:

- The UK (*Age Appropriate Design Code* 2020 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/)
- Ireland (Data Protection Commission 2021 https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf)
- The Netherlands (Ministry of the Interior and Kingdom Relations 2021 Code voor kinderrechten https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf)
- France (CNIL 2021 Les droits numeriques des mineurs https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs)
- Sweden (The Swedish Authority for Privacy Protection 2021 The Rights of Children and Young People on Digital Platforms https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf)

2. Welcoming the move away from industry-drafted co-regulation by default

We note that historically Code making processes have relied on industry drafting, through co-regulatory processes. These are deeply unpopular and problematic approaches.

Firstly, industry drafting fails to deliver Codes that function in children's best interests. The process of drafting the Online Safety Codes for Class 1A & 1B materials provided concrete examples of failures for children's safety in Australia. For example:

1. The age at which strong privacy protections must be offered is less than comparative requirements overseas. The Australian Codes for social media services set the age of private settings to 16, meaning that all under 16-year-olds have their accounts default to private when they first join a service. Under the UK's *Age Appropriate Design Code,*[13] or Ireland's F*undamentals for a Child-Oriented Approach to Data Processing,*[14] the minimum age is 18. This leaves Australian 16 & 17-year-olds significantly less protected.

   The *Online Safety Act* itself —in the unenforceable Basic Online Safety Expectations in the *Act* — expressed an intent for all children up until the age of 18-years-old to be protected by high privacy defaults. The Determinations states that "if a service or a component of a service... is likely to be accessed by children ... (an expectation is) ensuring that the default privacy and safety settings of the children's service are robust and set to the most restrictive level".[15] The Act defines a child as anyone up to the age of 18, as does the Determination. This means the industry-drafted Code falls short of the expectations laid out in the determination.

   This creates real risks for children. For example, private accounts prevent unwanted contact between children and adults. At Meta, they state for example *"Wherever we can, we want to stop young people from hearing from adults they don't know or don't want to hear from. We believe private accounts are the best way to prevent this from happening."*[16] This is backed by internal Facebook research leaked in the Facebook Files. The research suggests that Meta knew that recommending children to adult strangers as friends—via their People You May Know feature—drove 75% of grooming cases.[17] Private accounts 'turn off' the People You May Know feature. It is worth noting that the 'People You May Know' feature is still active on Facebook for Australian under 18 year olds where they are not private, as confirmed by Meta's head of safety to Australian parliament as recently as Sept 2024.[18] We acknowledge that these risks may not be explicitly around class 1A & 1B material which the Code targets, but clearly they are connected. If they were not, they would not have been included in the Code in the first instance. If they were worth

[13]UK Information Commissioner Office 2020 *Age appropriate design: a code of practice for online services* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/
[14]Ireland Data Protection Commission 2021 *Fundamentals For A Child-Oriented Approach To Data Processing* Fhttps://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
[15]Minister for Communications 2024 *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-bose-amendment-determination-2024.pdf, Schedule 1 Amendments, 3
[16]Meta 2021 *Giving young people a safer, more private experience on Instagram* https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/
[17]See slide 4, Leaked document 2021 *Friending and PYMK downstream Integrity Problems* https://www.documentcloud.org/documents/23322845-friending-and-pymk-downstream-integrity-problems
[18]Zoe Daniels 2024 'Meta's disregard for the public interest is 'galling', says independent MP Zoe Daniel' *The Australian* https://www.theaustralian.com.au/business/media/metas-disregard-for-the-public-interest-is-galling-says-independent-mp-zoe-daniel/news-story/7783e5551f8669f665c7599d4e1dc47c

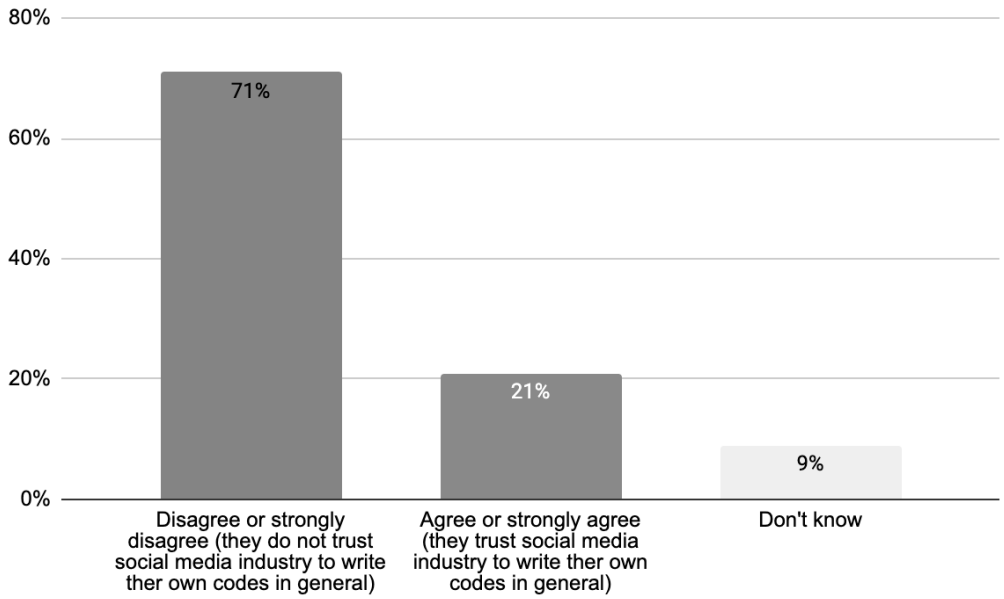
addressing in the Code, they were worth addressing properly and to the level expected in the *Online Safety Act*.

Appendix 1 highlights a legal opinion taking regarding the Online Safety Codes for Class 1A & 1B materials, which was drafted by industry through co-regulatory processes. It notes how the resulting codes included lower standards of default privacy protections than was intended by the *Online Safety Act* as a result of the co-regulatory process.

2. Likewise, protections for children's live location data (e.g. GPS data) are significantly weaker under the Australian Codes for social media than Codes developed elsewhere. Where the UK and Ireland, for example, prohibit the *collection* of children's live location data, the Australian codes prohibit *broadcasting* children's location data. Australians' data is already broadcast on average 449 times a day via the Real-Time-Bidding system,[19] which suggests that a lot of underlying location data is being unnecessarily collected about children. This creates risks for children. Data breaches, inappropriate accesses or even accidental publishing can happen where this data is being unnecessarily collected. Again, this is an example of industry-drafted Codes leading to lower levels of protection than regulator or legislator drafted Codes.

   These reduced protections must be understood as intentional rather than accidental. Many of the companies whose representatives drafted these Codes are offering stronger safety protections to young people overseas. An active decision was taken to set the safety standards in Australia's industry codes lower than 'best practice' in other countries they operate in.

Secondly, industry-drafted codemaking creates public trust issues with the regulatory processes. In Dec 2022, YouGov polled 1,508 Australians to explore their trust in co-regulation. Only 21% of adults suggested they trust the social media industry to write their own codes (see Figure 1). The majority said they would prefer if independent regulators drafted these codes, with 73% preferring the eSafety Commissioner draft the Online Safety Code (see Figure 2), and 76% preferring the Information Commissioner draft any potential privacy Codes for children (see Figure 3).[20]



[19]Irish Council of Civil Liberties 2024 *Australia's hidden security crisis* https://www.iccl.ie/wp-content/uploads/2024/07/Australias-RTB-security-crisis-report.pdf
[20]Reset.Tech Australia 2022 *How outdated approaches to regulation harm children and young people* https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/

Figure 1: People's response to the statement 'I trust the social media industry to write their own codes about online privacy and data protection in general' (n=1,508).

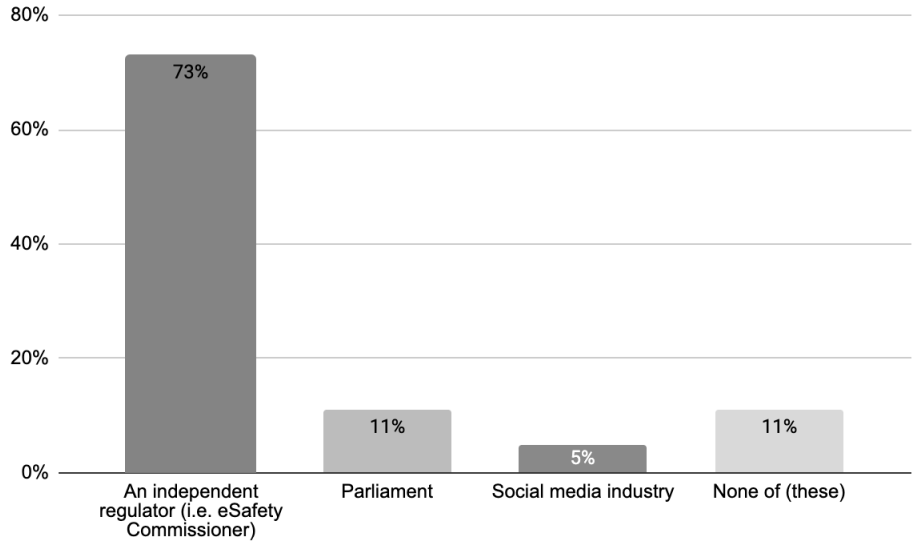


Figure 2: People's preference about who should write the codes for online safety for children (n=1,508) [If you had to choose, who would you most prefer to write the codes about online safety for children?]

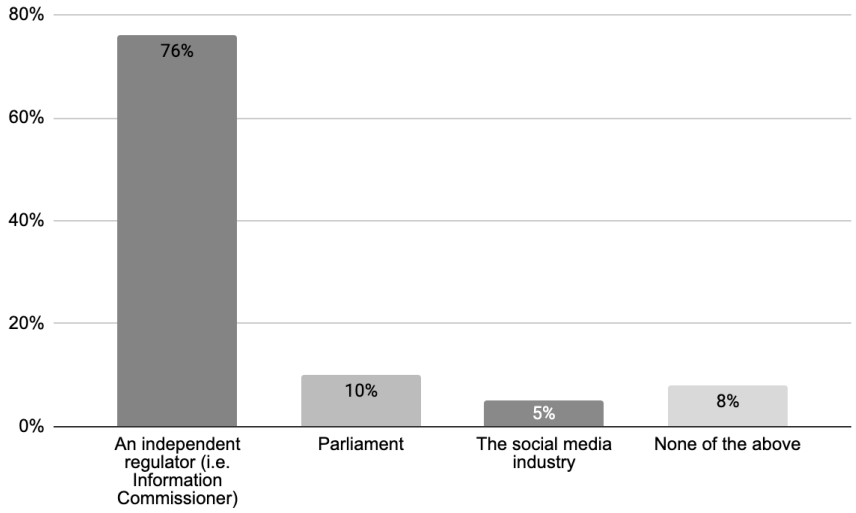


Figure 3: People's preference about who should write the codes for privacy safety for children (n=1,508) [If you had to choose, who would you most prefer to write the codes about online privacy for children?]

We have recently completed a policy roundtable exploring co-regulation and children's best interest. We will make a copy of the report available to the Committee as soon as feasible.

The powers provided for the OAIC to draft Codes directly are welcome, and must be maintained as the Children's Privacy Code is proposed.

3. The need for 'tranche two' of reforms as soon as possible

Many vital reforms were proposed in the *Privacy Act Review Report* and were agreed or agreed-in-principle by the Government.[21] Some of these are vital to ensuring Australia's privacy framework is fit for the digital era, especially including the updates to the definition of personal data and the inclusion of the fair and reasonable test for processing data. These will also affect children.

Further, many of the additional protections that will be delayed to tranche two also focus on children, such as a prohibition on targeting children, which has the capacity to be far more protective for children than a children's code. We are deeply disappointed to see that these vital reforms are not included in this first iteration of reforms.

However, we are cautious of 'perfect being the enemy of good' and believe that the Privacy and Other Legislation Amendment Bill 2024 propose some vital first steps that are necessary to updating Australia's privacy framework. We do not believe there is a reason to delay or impede the progress of these proposed reforms while we continue to advocate and push for further additional reforms.

Put simply, *we have already waited too long for these initial protections*. A child who turned 13 when civil society began calling for a privacy code in Australia (2021) will already be 18 by the time one is potentially implemented under this proposed timelines (2026). Childhoods do not wait for perfect proposals.

However, without some of these additional reforms, the effectiveness of a Children's Privacy Code will be significantly dampened. For example, it will not be able to offer protections for children's metadata and children's data will still be collected as part of the 'targeting pipeline'. We recommend a commitment to a firm deadline for the implementation of tranche two.

Conclusion and recommendations

The proposals presented in the Privacy and Other Legislation Amendment Bill 2024 are welcome first steps towards the broader changes needed in Australia's privacy framework. While we eagerly await tranche two of these reforms, these initial steps are welcome and should be swiftly implemented.

[21]Department of the Attorney General 2023 *Government Response | Privacy Act Review* Reporthttps://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

Appendix 1: Memorandum of legal advice re Online Safety Codes

Memorandum of legal advice

Date 8 October 2024

Subject Industry Codes registered by the e-Safety Commissioner under the *Online Safety Act 2021* (Cth)

Advice

1 Background

We have been asked to provide advice on:

1.1. Whether the *Social Media Services Online Safety Code (Class 1A and Class 1B Material* (**the Code**) registered under the *Online Safety Act 2021* (Cth) (**Online Safety Act**) offers less protection for 16 and 17-year old Australians than is expected under the *Online Safety (Basic Online Safety Expectations Determination) 2022* (**BOSE Determination**).

1.2. The implications of any inconsistencies or lesser protections.

2 Executive summary

In summary, our advice in relation to the above questions is:

2.1 Yes, the Code provides less protection for 16 and 17-year-olds than what is expected under the BOSE Determination in respect of default privacy and safety settings for services, or components of services, that are likely to be accessed by children. However, the BOSE Determination does not strictly mandate default safety settings for individuals under the age of 18.

2.2 The main implications of the inconsistency between the BOSE Determination and the Code are that 16 and 17-year-old Australians do not have default privacy and safety settings set to the most restrictive level and are consequently left vulnerable to a range of online harms including unwanted contact from strangers, sexual exploitation and grooming, and viewing unsolicited inappropriate content.

2.3 The current approach to the creation of Codes under the Online Safety Act enables industry stakeholders to prepare Codes that align with their commercial interests, rather than with the best interests of the child and children's online safety. Whilst we agree that industry should bear some responsibility for creating safer online spaces,[22] a simple way to ensure that Codes are consistent with the

[22]Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Amending the Online Safety (Basic Online Safety Expectations) Determination 2022 — Consultation paper, 22 November 2023, page 2.

intentions of the Online Safety Act and the BOSE Determination is to have those Codes prepared by the eSafety Commissioner following consultation with industry stakeholders.

3 Legislative framework and extraneous material

Online Safety Act

3.1. The Online Safety Act commenced on 23 January 2022. Its object is to improve and promote online safety for Australians: section 3.

3.2. Pursuant to section 45(a) of the Online Safety Act, the Minister may, by legislative instrument, determine that the basic online safety expectations for a social media service are the expectations specified in the determination.

3.3. A determination made under section 45 does not impose a duty that is enforceable by proceedings in a court: section 45(4).

3.4. Class 1 material and Class 2 material is defined in sections 106 and 107 respectively and apply to films, publications, computer games and any other material.

3.5. In addition to the provisions allowing the Minister to make determinations, the Online Safety Act also provides a mechanism for industry associations to develop codes (**industry codes**) to protect Australians from class 1 and 2 material: Part 9, Division 7 of the Online Safety Act. Under section 141, if the Commissioner is satisfied that a body or association represents a particular section of the online industry, the Commissioner may, by written notice given to the body or association, request the body or association to develop and industry code that applies to participants in that section of the industry.

3.6. Section 140 outlines the process for the registration of industry codes which, amongst other things, requires the Commissioner to be satisfied that, where the code deals with one or more matters of substantial relevance to the community, the code provides appropriate community safeguards for that matter or those matters: section 140(1)(d)(i).

The BOSE Determination

3.7. The BOSE Determination was made under section 45 of the Online Safety Act and specifies basic online safety expectations for a social media service, a relevant electronic service of any kind, and a designated internet service of any kind.

3.8. Subsections 6(1), (2) and (2A) of Division 2 of the BOSE Determination require the provider of services to take reasonable steps to: ensure that end-users are able to use the service in a safe manner; proactively minimise the extent to which material or activity on the service is unlawful and harmful; and ensure 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.

3.9. Subsection (2A), of the BOSE Determination, which requires service providers to 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, was inserted by the *Online Safety (Basic Online Safety*

Expectations) Amendment Determination 2024[23] (**the amending instrument**) with effect from effect from 31 May 2024.

3.10. Subsection 6(3) provides a non-exhaustive list of examples of reasonable steps that could be taken and relevantly includes that if a service or a component of a service (such as an 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 set to the most restrictive level: subsection 6(3)(b).

3.11. The Explanatory Statement accompanying the amending instrument[24] states the following in relation to the purpose of the BOSE Determination:

> It is not intended that the Commissioner prescribe specific steps for service providers to take to meet the expectations. The Determination itself also does not prescribe how expectations will be met. This is intended to provide the highest degree of flexibility for service providers to determine the most appropriate method of achieving the expectations.
>
> Notwithstanding that the Determination provides flexibility for service providers, it does outline a number of examples of reasonable steps that could be taken within the sections of the Determination. Not all reasonable steps have to be taken by all service providers. Rather, they are intended to provide guidance to service providers.

3.12. In relation to the 'reasonable steps' listed in subsection 6(3) of the BOSE Determination, the Explanatory Statement states:

> The Determination provides flexibility for service providers to uplift online safety practices in a way that works for them. A number of examples of reasonable steps that could be taken are included within the Determination to provide guidance to service providers about what actions could be taken that could lead to compliance with the provisions. These reasonable steps do not necessarily have to be taken in order for a service provider to comply with the Determination.

3.13. The Statement of Compatibility with Human Rights in the Explanatory Statement relevantly explains that (emphasis added):

> The provisions of the Determination are directed towards protecting the preservation of privacy and reputation of vulnerable people. For example, the provisions at Paragraph 6(3)(b) provides that the most restrictive default privacy and safety settings be provided **on a service or component of a service that is targeted at, or being used by, children**.
>
> …
>
> The Determination supports the best interests of the child by including provisions that provide guidance to social media services, relevant electronic services and designated internet services to ensure default privacy and safety settings **on children's services**. Provisions in the Determination expect service providers to ensure that the default privacy and safety settings of children's services (a service or a component of a service that is targeted at, or being used by, children) are set at the most restrictive level…

3.14. Attachment A to the Explanatory Statement further explains (emphasis added):

[23] https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-bose-amendment-determination-2024.pdf

[24] F2022L00062ES

> Subsection 6(3) provides examples of reasonable steps that could be taken to guide service providers on what actions they could choose to undertake that would enable them to meet the expectations outlined in Subsection 6(1) and Subsection 6(2). The list under Subsection 6(3) is not exhaustive, and service providers may elect to take different steps to meet the expectations in a way that best suits their circumstances.
>
> …
>
> Paragraph 6(3)(b) suggests that service providers could meet the expectations in subsections 6(1) and 6(2) by **ensuring that default privacy and safety settings of a service that is targeted at, or being used by, children are set at the most restrictive level**. This example of a reasonable step that could be undertaken is purposefully flexible to allow the provider of a service to determine, in consultation with the Commissioner (under Section 7), what a 'most restrictive' level means for their service. The intent of this reasonable step is to protect children from harm.

Social Media Services Online Safety Code (Class 1A and Class 1B Material) (**the Code**)

3.15. On 16 June 2023, the *Social Media Services Online Safety Code (Class 1A and Class 1B Material)* (**the Code**) was registered by the eSafety Commissioner under the industry code provisions in the Online Safety Act. The Code applies to a provider of social media services, so far as materials on that service are provided to Australian end-users: section 2.

3.16. The Code deals with class 1A and class 1B material. Class 1A material is material that is seriously harmful and generally should not be accessible online, whilst class 1B material is also harmful but may be appropriate for adults to access provided suitable limitations are in place.[25]

3.17. Section 4 of the Code outlines the risk profile for various social media services. It specifies that, how the Code is to be applied, depends on the risk posed to Australian end-users that class 1A and 1B material will be accessed, distributed or stored on that service. Subject to some exceptions, a provider of a social media service must undertake a risk assessment to assess the risk posed to Australian end-users and must determine that the risk profile of the social media service is either Tier 1, Tier 2 or Tier 3: subsection 4.1 of the Code. A Tier 1 social media service is the highest risk profile.

3.18. Section 7 of the Code outlines compliance measures for class 1A and class 1B material to achieve the specific objective of requiring industry participants to take reasonable and proactive steps to create and maintain a safe online environment for Australian end-users.

3.19. Part 7 of section 7 provides minimum compliance measures for Tier 1 social media services and states that:

> A provider of a Tier 1 social media service that permits a young Australian child to hold an account on the service must at a minimum:
>
> (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

[25] eSafety Commissioner, *Phase 1 Industry Codes (Class 1A and Class 1B Material) - Regulatory Guidance*, December 2023 (https://www.esafety.gov.au/sites/default/files/2023-12/Phase-1-Industry-Codes-%28Class-1A-and-Class-1B-Material%29-Regulatory-Guidance.pdf?v=1726702819720)

(b) easy to use tools and functionality that can help safeguard the safety of a young Australian child using the service.

3.20. Section 143 of the Online Safety Act provides that the Commissioner may, by written notice, direct a person to comply with an industry code if satisfied that the industry code has been contravened. A person must comply with a direction under subsection 143(1): subsection 143(2). Contravention of subsection 143(2) attracts a civil penalty of 500 penalty units.

Definitions of 'child'

3.21. The Online Safety Act, BOSE and Code contain the following definitions of the term '*child*':

(a) the Online Safety Act defines '*child*' as '*an individual who has not reached 18 years*': section 5;

(b) the BOSE does not expressly define '*child'*, but the Explanatory Statement suggests that it adopts the same definition as that used in the Online Safety Act;[26] and

(c) the Code defines an '*Australian child*' as '*an Australian end-user under the age of 18 years*' and a '*Young Australian child*' as an '*Australian end-user under the age of 16 years*': sections 3.3 and 3.4.

4 Does the Code offer less protection for 16 and 17-year-old Australians than what is expected under the BOSE Determination?

4.1 With reference to [9]-[10] of your request for advice, we understand that you consider:

(a) the BOSE Determination requires default privacy and safety settings for all Tier 1 social media services to be set to the most restrictive level for all children under the age of 18; and

(b) the Code's minimum compliance measures for default privacy settings as outlined at [3.19] above leaves 16 and 17-year old Australians unprotected because it imposes minimum requirements in respect of default settings for 'young Australian children' only (i.e., children aged under 16).

4.2 A plain reading of subsection 6(3)(b) of the BOSE determination does not indicate that it requires default privacy and safety settings to be set to the most restrictive level for all children under the age of 18 because the use of the word 'could' instead of 'must' indicates that implementation of the reasonable steps listed in subsection (3) is discretionary.

4.3 As outlined at [3.11]-[3.13] above, the Explanatory Statement to the amending instrument makes clear that subsection 6(3) of the BOSE Determination does not impose any specific requirements on social media service providers in terms of the reasonable steps that need to be taken to ensure that the requirements in subsections 6(1), (2) and (2A) are met. The list of 'reasonable steps' in that provision is intended to provide guidance only, and social media service providers do not have to implement them in order to comply with the BOSE Determination.

[26] Minister for Communications 2024, *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* (https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-bose-amendment-determination-2024.pdf)

4.4 Further, subsection 6(3)(b) refers to 'children's services', not children. In our view, its focus appears to be ensuring that default privacy and safety settings are set to the most restrictive level for services, or a component of a service that are likely to be accessed by children.

4.5 Even if the BOSE Determination did require strict compliance with subsection 6(3)(b), the Explanatory Statement to the amending instrument suggests this would oblige social media service providers to ensure that default privacy and safety settings of any service, or component of a service, that is 'targeted at, or being used by, children' be set at the most restrictive level for children aged 16 and 17 and adults (i.e., for all users). On that basis, we consider the Code provides a lesser standard of protection than that expected under the BOSE Determination, specifically, because it does not afford individuals aged 16 and 17 years the benefit of default privacy and safety settings on services that permit children under the age of 16 to hold an account.

4.6 Although it is unclear what constitutes 'a service, or a component of a service that is likely to be accessed by children', a service that permits 'young Australian children' as defined in the Code to hold an account would very likely meet the criteria. In the absence of a mandatory age verification mechanism, the most practical way to ensure that all children using 'a service, or a component of a service that is likely to be accessed by children' are afforded the benefit of having their default privacy and safety settings set to the most restrictive level may be to ensure that everyone who accesses the service has those protections.

5 The implications of any inconsistencies or lesser protections

5.1 As a consequence of the inconsistency between the Code and the BOSE Determination, certain safety measures are only mandated in respect of 'young Australian children' as defined in the Code. This means that the protections and safeguards applied to Australian children under the age of 16 — including preventing unwanted contact from unknown users and the location of the child being shared through default privacy settings — are not required for 16 and 17-year old Australians who access social media services that permit a young Australian child to hold an account on the service.

5.2 The recent announcement of the introduction of 'teen accounts' on Instagram provides a useful example of this lesser protection in practice. On 17 September 2024, Instagram shared that 'teen accounts' would be introduced globally in early 2025 and would include default private accounts for all teens under 16 (including those already on Instagram and those signing up) and teens under 18 'when they sign up for the app'.[27] The lack of any mandate in the Code for default privacy settings to apply to 16 and 17-year olds means that it is consistent with and permitted by the Code for the privacy settings of existing Instagram users over the age of 16 to remain unchanged and for new users over 16 to change their privacy settings to public without a parent's permission.

5.3 In the absence of default privacy settings, 16 and 17-year old Australians can be contacted by people they do not know, tagged in posts by people they do not follow, exposed to inappropriate content, and identified by strangers via 'people you may know' functions. Given some of the most common negative online experiences for young people relate to receiving repeated unwanted online messages, being sent inappropriate content involving pornography or violence, and being contacted by strangers,[28] the lack of any requirement under the Code

[27] https://about.instagram.com/blog/announcements/instagram-teen-accounts.

[28] Office of the eSafety Commissioner, *State of Play - Youth, Kids and Digital Dangers* (3 May 2018) page 20-21.

for default privacy settings for Australians aged 16 and 17 presents a real risk to the safety of this group online.

5.4 Having regard to the object of the Online Safety Act and the requirements in subsections 6(1), (2) and (2A) of the BOSE Determination, we consider that extending the protections that are available to 'young Australian children' under the Code to 16 and 17-year olds is the desirable and preferable approach when regard is had to the potential harms that can occur in the absence of default privacy and safety settings.