Does **digital co-regulation** *function in* ***children's best interests?***

October 2024

POLICY BRIEFING

Reset·Tech
AUSTRALIA

The default reliance on industry co-regulation must be critically interrogated.

*There are **limited real world contexts** where co-regulation is likely to produce outcomes that advance children's rights and function in their best interests.*

Reset·Tech
AUSTRALIA

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

https://au.reset.tech/

COVER ARTWORK: Digital collage composed of archival images sourced from: Library of Congress/Google Books/ Pinterest/Flickr/New York State Archives

Contents

Introduction

There is a paradox in Australian digital regulation: as the competition and consumer harms of the technology sector began to escalate, 'direct regulation' was overshadowed by self-regulatory, quasi-regulatory or co-regulatory preferences. Presumably, this shift was encouraged by movements like Regulatory Impact Analysis, measures designed to 'protect business from new, unnecessary regulation'.[1] It is arguable that Australia's embrace of deregulation was not intended to become a shield from which the world's largest and most powerful digital companies now appear to benefit.

This policy briefing reflects discussions held at a roundtable of 13 experts from academia and civil society in October 2024, where we explored the specific outcomes of digital co-regulation on Australian children and young people, and queried whether co-regulation can function in their best interests. The event was held under the Chatham House Rule, meaning this briefing presents an overview of the discussion, without attributing comments made.

Co-regulation is not a new concept in Australia. It means that industry develops and administers the rules, while the government provides legislative backing to enable enforcement.[2] Co-regulation is particularly prevalent in the broadcasting and telecommunications sectors. Key examples include the Telecommunications Consumer Protections Code and the Commercial Television Industry Code of Practice 2015.[3] Given the structural and seismic differences between telecommunications providers (such as TV and radio) and foreign digital platform behemoths, it appears that the co-regulatory concept has surpassed the more confined sectoral context in which it was designed to operate.

The Australian Law Reform Commission wrote comprehensively about the factors determining regulatory reforms in 2011. The guiding instrument at the time was the Australian Government Best Practice Regulation Handbook. The principles are clear: direct government regulation should be considered for high-risk, high-impact and high-significance issues. Self-regulation or co-regulation may be feasible if there is 'no strong public interest concern', the risks are low, and the market can self-correct.

The Australian Government Best Practice Regulation Handbook states that direct government regulation should be considered when, among other things: the problem is high-risk, of high impact or significance; the community requires the certainty provided by legal sanctions; and there is a systemic compliance problem with a history of intractable disputes and repeated or flagrant breaches of fair trading principles, with no possibility of effective sanctions.

On the other hand, self-regulation—or by extension, more co-regulation—may be a feasible option if: there is no strong public interest concern, in particular no major public health and safety concerns; the problem is a low-risk event, of low impact or significance; and the problem can be fixed by the market itself—for example, if there are market incentives for individuals and groups to develop and comply with self-regulatory arrangements.[4]

The tendency towards deregulation continues with gusto, yet the scale of public harms and systemic risks from digital platforms has surged. Given the litany of public scandals surrounding large technology companies and an inherent hostility to regulation and compliance, it is curious to observe the flawed yet persistent reflex for self regulation and co-regulation.[5] Particularly in light of the noise surrounding social media harms and online safety throughout 2024, it seems especially discordant that federal and state governments are sounding the alarm for serious tech regulation yet avoiding 'finishing the job' of conducting that regulation directly.

Digital co-regulation: The case of online safety's industry codes

The *Online Safety Act* 2021 empowers the eSafety Commissioner with the challenging task of supervising the development of industry online safety codes.[6] A steering group of industry associations, typically represented by the Digital Industry Group Inc and the Communications Alliance, is responsible for the drafting.[7] Rich anecdotes from the 'Phase 1' code development process suggest it involved unique conditions of inflaming industry and exhausting public interest representatives. Academic experts Karen Lee and Derek Wilding[8] note a 2020 departmental report that appears to anticipate these dynamics:

> *The code development process has appeared to suit matters that require cooperation across industry (e.g. technical matters), rather than consumer issues that may create an impost on industry. There is an inherent tension in a process that requires industry to formulate its own consumer protection rules.*[9]

Beyond the impressions of and experiences with the process, it also generated substandard outcomes. As discussed in this paper, one specific example involves the establishment of a lower age standard for default privacy protection than was potentially intended (16 years old rather than 18 years old). This occurred despite warnings from civil society during the code drafting process,[10] inviting the question:

Is confining public interest feedback to an easily dismissed stakeholder category, in a process run by industry, really the way forward here?

A shift to regulator drafting

There are key developments suggesting that the era of industry drafting and digital co-regulation is slowly coming to an end. For the critical issues of children's privacy and data protection, and scam prevention, the bills currently before Parliament propose the respective regulators or departmental bodies draft the codes.[11]

We propose that direct regulation should be re-entrenched as the primary preference for regulating large digital platform companies in Australia.

This memo summarises the discussions held and proposes some recommendations for Australia's policy decision-makers. The event included three provocations, which are summarised in the following pages, along with an overview of the broader discussion.

1. The children's best interests principle and co-regulation

There are three key reasons to be interested in adopting a rights-based assessment model:

1. A rights-based assessment model might be persuasive option because:
   - Australia has an international obligation to comply with standards under the United Nations Convention on the Rights of the Child (albeit not binding)
   - The federal government has an obligation to consider international human rights frameworks when developing legislation under the *Human Rights (Parliamentary Scrutiny) Act 2011*
2. A rights-based assessment is more comprehensive than a reliance on 'best interests' in offering insights and guidance into the appropriate processes and standards required when seeking to protect the privacy of children. A rights-based assessment avoids some of the limitations associated with the application of the best interests principle, such as it can be indeterminate, and it can serve as a proxy for the interests of others.
3. A rights-based assessment model requires balancing participation and protection of rights of children.

However, the 'best interests' principle remains important within a rights-based model. The 'best interests' principle is a guiding principle of a rights-based approach, indeed it emerges from Article 3 of the Convention on the Rights of the Child.[12] There is also a significant body of evidence regarding its importance; for example General Comment 14[13] and General Comment 25 on *Children's Rights in Relation to the Digital Environment*[14] rest on the best interests principle.

A rights-based approach allows us to reduce the indeterminacy of 'best interests' by offering a model for its interpretation.

That is:

- Best interests must be informed by and be consistent with the other rights under the Convention on the Rights of the Child
- Best interests must be informed by relevant and available evidence (e.g. what evidence do we have about effective regulatory codes?)
- Best interests must be informed by the views of affected children themselves, and their participation
- Best interests must also be informed by those who have care and responsibility for children (such as parents, carers, and educators)
- Best interests can apply to groups of children or individual children

A rights-based approach requires a range of measures to ensure effective protection of a child's privacy and mandates all appropriate measures be taken for their protection. This includes legislative, social and educational measures, and requires reflection on the appropriateness and effectiveness of these measures. The Committee on the Rights of the Child stresses the need to protect children's rights through regulation but does not address nor specify what kind of regulatory model would be appropriate. However, it outlines that regulation must be guided by principles and evidence.

A rights-based approach also includes procedural (instrumental) and substantive (normative) elements. In terms of procedural elements, it requires a focus on *participation* in processes:

- A rights-based approach requires children's participation, noting that co-design is very different from co-regulation. It raises questions about who controls or directs the process
- It requires developing legislation and policies in ways that involve all children and listens to their needs
- There is an inherent challenge in this, as the implementation of participation can be tokenistic or substantive. Moving beyond tokenistic participation is a challenge
- To be 'responsive', co-regulation would require the participation of consumers to be effective and legitimate
- There are significant barriers to participation in co-regulatory products (whether in complaints or submissions for development. These processes are often reactive, and other models to maximise participation, such as focus groups, surveys, and round tables, are not always implemented. These challenges are heightened for children as they face greater obstacles to participation
- Children's meaningful participation, as described in Article 12 of the United Nations Convention on the Rights of the Child requires rethinking participatory methods for children so they are proactive rather than reactive
- Participation must be relevant and voluntary, with measures that encourage involvement in line with the age and maturity of participants; must be transparency and accountability regarding how data and inputs gathered will be used
- Potentially, a rights-based approach also requires consultation with parents, carers, teachers, other actors and civil society

In terms of substantive elements, it requires scrutiny, compliance, monitoring and evaluation:

- A co-regulatory model also emphasises the need for consultation, but this is not sufficient under a rights-based approach. Under a rights-based approach an assessment of whether the proposed code is consistent with children's human rights is also necessary
- The Committee on the Rights of the Child discusses the idea of a child rights impact assessment and emphasises the need for a coordinating body within government to ensure all policies are consistent with children's rights
- They also stress the importance of independent monitoring of policies to ensure compliance with the Convention on the Rights of the Child, with the capacity for effective complaints, remedies, monitoring and evaluation
- Under this approach, there may be a need for a mechanism to facilitate and/or scrutinise any code produced by a co-regulatory process to ensure it is consistent with children's rights before being approved

Lastly, a rights-based approach creates both a need for education and a special role for civil society. Specifically, there is an explicit obligation to train businesses about children's rights and how their work will impact on these rights, as well as an obligation of due diligence. This is in line with the Business and Human Rights Framework.[15] There is also an explicit obligation to involve civil society in ensuring that both the process and outcomes of any consultative process is consistent with the Convention on the Rights of the Child.

2. The outcomes of co-regulation in safety codes and children's best interests

The online safety framework has recently developed a series of codes through industry drafting, specifically the Online Safety Codes for Class 1A and Class 1B materials.[16] There are some lessons from that process that are worth reflecting on.

1. The age at which strong privacy protections must be offered is lower than comparative requirements overseas.

The Australian Online Safety Codes for Social Media Services set the age of private settings at 16, meaning that all under 16-year-olds have their accounts default to private when they first join a service. In contrast, the UK's *Age Appropriate Design Code,*[17] and Ireland's *Fundamentals for a Child-Oriented Approach to Data Processing,*[18] set the minimum age to 18. Evidently, Australian 16 & 17-year-olds are significantly less protected.

The substantively unenforceable Basic Online Safety Expectations — developed under the *Online Safety Act*— express an intent to protect all children up until the age of 18-years-old with high privacy defaults.[19] Furthermore, the amending Ministerial Determination from earlier this year 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".[20] 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 outlined in the Determination.

This inconsistency creates real risks for children. For example, private accounts prevent unwanted contact between children and adults. At Meta, they state, *"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."*[21] This is supported by internal Facebook research leaked in the Facebook Files, which suggests that Meta knew recommending children to adult strangers as friends—via their 'People You May Know' feature— drove 75% of grooming cases.[22] 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 users under 18 whose accounts are not toggled to the 'private' setting, as confirmed by Meta's head of safety to Australian parliament as recently as September 2024.[23] We acknowledge that these risks may not be explicitly around Class 1A and Class 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 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 than those developed elsewhere.

For example, while the UK and Ireland prohibit the *collection* of children's live location data, the Australian codes only prohibit *broadcasting* children's location data. Australians' data is already broadcast on average, 449 times a day via the Real-Time Bidding system,[24] suggesting that a substantial amount of underlying location data is being unnecessarily collected about children. This creates risks for children, as data breaches, inappropriate access, or even accidental publishing can occur when this data is unnecessarily collected. Again, this exemplifies how industry-drafted codes lead to lower levels of protection than those drafted by regulators or legislators.

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 made to set the safety standards in Australia's industry codes lower than 'best practice' in other countries where they operate.

Furthermore, industry-drafted code-making creates public trust issues with regulatory processes. In December 2022, YouGov polled 1,508 Australians to explore their trust in co-regulation, and found that:

- Only 21% of adults indicated they trust the social media industry to write its own codes
- The majority expressed a preference for independent regulators to draft these codes, with 73% favouring the eSafety Commissioner to draft online safety codes, and 76% preferring the Information Commissioner to draft any potential privacy codes for children.[25]

Lastly, young people themselves express a desire for a more active role in developing codes and regulatory frameworks than what industry drafting allows for. Young people have been actively engaged in describing what they want from, for example, an online privacy code.[26]

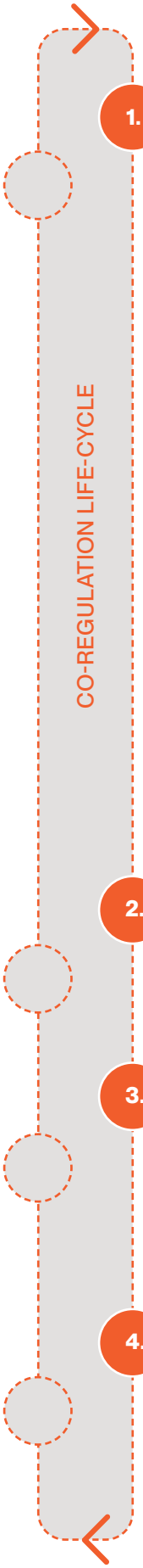
3. Developing communications regulation to harness industry expertise and ensure good public policy outcomes

In the realm of digital regulation, co-regulation entices policy decision makers. The promise of co-regulation is that governments can leverage industry-specific knowledge, and benefit from more cost-effective solutions. The argument suggests that by encouraging industry to take greater control of its practices, digital platforms will directly participate in rule formation, which, in turn, raises levels of compliance.

However, this narrative is not the full story, and co-regulation is not without its drawbacks. There is a risk of collusion and regulatory capture, which can lead to weaker standards that may ultimately harm public interest.

In this context, are there circumstances where co-regulation could work?

The success of co-regulation depends on several preconditions. In Australia, there has been limited academic exploration of a co-regulatory approach in this environment, although an ARC-funded project is currently exploring it. In the absence of a definitive answer, bodies such as the UK Office of Communications[27] and ACMA[28] have highlighted a range of contextual factors necessary for effective regulation. These factors include heightened sensitivity to consumer needs,[29] and a clear stance on key issues such as privacy, transparency and accountability.



As such, it is helpful to adopt a **life-cycle approach to co-regulation**, which breaks down the component parts of co-regulation:[30]

1. Rule-making:

- Empirical studies suggest that the timing of rule-making matters. Robust code development is more likely to occur in times of perceived industry crisis or in times of media scrutiny over key issues. However this needs constant review. A co-regulatory approach is not a 'set and forget' approach to policy. It needs ongoing political involvement.
- Ensuring that high standards are maintained throughout the rulemaking process is challenging. Co-regulatory rulemaking often results in a levelling down of standards, as the least able participant tends to dictate the content of the code because providers will not sign up when others cannot comply with it. Codes are therefore more likely to set regulatory floors rather than encourage behaviour that goes beyond compliance.
- Regulatory oversight and engagement are essential during the rule-making process. Close attention must be paid to the composition of code-making. When registering codes, regulators should have the authority to remove weaker provisions and maintain stronger ones. Regulators should not be placed in a position where the testing for code regulation resembles a 'take it or leave it' approach. The framework outlined in the recent Combatting Misinformation and Disinformation Bill represents steps in the right direction, as ACMA gains the ability to veto provisions of the misinformation code (see s 51 of the Bill).
- In addition, there must be broader consultation to ensure a wide range of views is considered not only from civil society but also from consumers. It is crucial for consumers to have a seat at the table from early stages of regulation formation, prior to settling the main ideas. The opportunity to submit written feedback is too late, as ideas are typically already framed by then, and established agreements have been made during the preceding process leading up to written consultations.

2. Compliance:

- Compliance does not happen in the dark and there is a clear need for greater transparency and reporting from co-regulators to keep them accountable. While important work has been done in this area relating to telecommunications, similar stances are needed in the Australian context.

3. Enforcement:

- There is a need for regulators to have strong enforcement powers and a review to ensure that regulators remain involved and accountable. In Australia there seems to be an aversion to 'naming and shaming' organisations that fail to comply with the rules, and it appears that not all code enforcement decisions are publicly available, leading to calls for enforcement registers so academics and others can better track regulatory decision-making over time.[31]

4. Review:

- Codes need indicators and measures built into them, to help assess the impact of the code. In the absence of this, the success of a code is often measured by the number of complaints made, which is an oversimplification. While a reduction in complaints can be one measure of success, it should not be the only one. Relying on this metric alone oversimplifies the analysis of whether a code is truly effective.

Discussion

The discussion focused on 2 key themes.

1. **Effective regulation for children and young people needs to reflect both children's rights and consumer protections.**

Children and young people are an interesting case study to explore the capacities of different regulatory models because they exist at the crossroads of various legal and social frameworks.

From a consumer rights perspective, children and young people are consumers and potentially vulnerable ones. Consumer protections are—rightly—paternalistic in their framing precisely because they aim to protect consumers from harm. This is evident in the shift away from relying on consumer consent to justify poor business practices; we do not want a system where complex safety and privacy decisions are hoisted onto consumers to navigate alone. Consumer protections embrace a paternalistic approach precisely to address the imbalances between consumers and businesses, which is especially relevant when we are talking about very large tech companies and teenagers.

From a child rights perspective, a paternalistic approach to children can be complicated. It may help advance children and young people's rights to protection, but it may undermine their rights to participation and access. We see this play out in debates around, for example, 'banning children' from social media. An overreliance on paternalism may undermine children's right to participation, to have a meaningful say, (and also in the case of social media bans, to access).

The word 'co-regulation' suggests there should be more space for children and young people to engage, but this is not necessarily what we are seeing. Co-regulation is not co-design as we understand it in the child rights world. It is not a rights-based approach, and it is hard to see how children's voices could be placed on a level playing field with industry voices as the current drafting processes stands. It would require a massive shift – in digital regulation, but also in policy making in general. Overall, Australia fails to recognise that children and young people have insights and understandings on how to contribute to policies that affect their lives.

Getting the balance right, and embracing a child rights and consumer protection approach is critical to developing digital policy that is 'in children's best interests'. It is unclear if industry drafting or co-regulatory approaches, in general, are nuanced enough to achieve this. (Indeed this is difficult enough to achieve in policymaking overall, as discussed below).

Two key barriers to tackling this complexity were discussed:

1. A lack of awareness regarding the impact of co-regulation on digital policy for children and young people. The need to, and value of, engaging children and young people in policymaking, particularly digital policymaking, is rarely recognised. When this deficiency is layered on top of industry-drafting processes, clear gaps emerge. However, this is an emerging space, and there are some academics, civil society organisations and policymakers entering this discussion now, which offers some optimism for greater visibility of these issues.
2. A lack of adequately resourced advocates for children's rights in this space. Both civil society and children's advocates are not sufficiently resourced to provide an adequate counterbalance, nor to hold the space necessary for children to participate effectively.

It is difficult, but that certainly does not mean we should not try.

---

2. The need for a re-muscularisation of policymaking capacity

There is a need for a broader 're-muscularisation' of policymaking in general, but particularly in digital policymaking areas. Twin dynamics hamper contemporary policy. First, Australia faces a progressively slimmed down public service. Regulatory efforts have also been broadly hampered by departmental 'efficiency dividends' which have left the public service short of necessary, specialised expertise. Second, this has led to a normalisation of 'contracting out' policy work. Departments have struggled – usually for sensible and justifiable reasons – to provide sufficient expertise on policymaking outcomes. This has resulted in policy consultation processes where policy has effectively been written by private sector consultants, especially the Big Four, without sufficient regard for potential conflicts or capture. Even industry has been critical of these processes. These dual dynamics have contributed to an overreliance on industry self-regulation.

There are multiple policy contexts where these dynamics have led to significant failures:

- The lessons learned from Robodebt are that policymakers need to be in a position to provide frank, fearless advice, rather than relying on senior figures whose salaries are contingent on a government contract.
- The development of broadcasting codes in this context has generated low levels of compliance, with disappointing enforcement options available. Formal warnings have largely been 'off the table' because the codes are voluntary standards, and compulsory notices to comply are few and far between.

Despite the government's willingness to pursue policy reform around digital communications issues, especially in novel areas of regulation, they face significant capacity challenges. For example, well-intentioned attempts at legislation on novel issues such as misinformation and disinformation have suffered from capacity constraints around advancing vital, technical adjustments, as well as a generally poor public understanding of the regulatory framework. The risks and harms to the public created by digital platforms' products and services urge a fulsome public policy response with the confidence to recognise where approaches are not working and adapt new ones that do.

Recommendation

The default reliance on industry co-regulation must be critically interrogated. There are *limited real world contexts* where co-regulation is likely to produce outcomes that advance children's rights and function in their best interests.

Effective policymaking may need to move beyond its overreliance on industry drafting, which requires sufficientre-muscularisation, re-skilling and re-resourcing of the public sector.

Endnotes

1 OECD 2010 *Review of Regulatory Reform: Australia Towards A Seamless National Economy* https://www.oecd-ilibrary.org/docserver/9789264067189-en.pdf, 15

2 Australian Law Reform Commission 2011 *National Classification Scheme Review: Discussion Paper* https://www.alrc.gov.au/wp-content/uploads/2019/08/dp_77_whole_pdf_.pdf, 191

3 For a detailed list of self-regulatory and co-regulatory schemes in the communications sector, see Karen Lee and Derek Wilding 2020 *Engaging the Public In Codes of Practice* https://opus.lib.uts.edu.au/bitstream/10453/140353/2/IM-April-2020-Vol-48-Issue-1_Lee-and-Wilding.pdf, 25

4 Australian Law Reform Commission 2011 *National Classification Scheme Review: Discussion Paper* https://www.alrc.gov.au/wp-content/uploads/2019/08/dp_77_whole_pdf_.pdf, 191

5 Rys Farthing and Dhakshayini Sooriyakumaran 2021 *'Why the era of Big Tech self-regulation must end' Australian Quarterly* https://www.jstor.org/stable/27060078

6 *Online Safety Act 2021*, s 141

7 'OnlineSafety.org.au' 2024 *About Us* https://onlinesafety.org.au/#ABOUT

8 Karen Lee and Derek Wilding 2022 'The case for reviewing broadcasting regulation' *Media International Australia* 182(1), pp. 67-80, quoting the *Australian Government's Consumer Safeguards Review* (2020) https://www.infrastructure.gov.au/sites/default/files/documents/consumer_safeguards_review_2020_part_c_august2020.pdf

9 Department of Infrastructure, Technology, Regional Development and Communications 2020 *Consumer Safeguards Review—Part C—'Choice and Fairness' Consultation Paper* https://www.infrastructure.gov.au/have-your-say/consumer-safeguards-review-consultation-part-c-choice-and-fairness

10 See Reset.Tech Australia 2023 *Submission to the Online Safety Codes Consultation* (https://onlinesafety.org.au/wp-content/uploads/wpforms/31-9e10405917e4c106ebe4ec5e69a7bc86/Reset.Tech-Australia-Revised-Codes-Reset-Submission-Google-Docs-869c0da1775d8d037a97bb1a1db860d5.pdf) as well as the Australian Child Rights Taskforce (ACRT 2023 *Submission to the Online Safety Codes Consultation* https://onlinesafety.org.au/wp-content/uploads/wpforms/31-9e10405917e4c106ebe4ec5e69a7bc86/ACRT-submission-to-the-Revised-Online-Safety-Codes-March-2023-aa7fb069cf093dc4ef7ad245ec3423aa.pdf)

11 The Privacy and Other Legislation Amendment Bill 2024 proposes for the Children's Online Privacy Code to be drafted by the Office of the Australian Information Commissioner. In the Treasury Laws Amendment Bill 2024, the Scams Prevention Framework proposes powers for a Treasury Minister to make a Scams Preventions Framework (SPF) code for a regulated sector.

12 United Nations 1989 *Convention on the Rights of the Child* https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

13 United Nations 2013 *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration* https://www.refworld.org/legal/general/crc/2013/en/95780

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

15 UNOHCHR 2011 *Guiding Principles on Business and Human Rights* https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

16 Communications Alliance & DIGI 2023 *Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material)* https://onlinesafety.org.au/wp-content/uploads/2023/06/230616_1_SMS-Schedule_REGISTERED-160623.pdf

17 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/

18 Ireland Data Protection Commission 2021 *Fundamentals For A Child-Oriented Approach To Data Processing* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

19 The point on enforceability is distinct from recent litigation outcomes between the regulator and X Corp, which pertain to non-compliance with transparency notices. While platforms may face enforcement actions for failing to comply with regulator requests for information, this does not equate to being held accountable for the substance of their safety measures.

20 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

21 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/

22 See slide 4, Leaked document 2021 *Friending and PYMK downstream Integrity Problems* https://www.documentcloud.org/documents/23322845-friending-and-pymk-downstream-integrity-problems

23 Zoe Daniel 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

24 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

25 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/

26 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/

27 Ofcom 2008 *Identifying appropriate regulatory solutions: principles for analysing self- and co-regulation* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/8466-coregulation/statement/statement-identifying-appropriate-regulatory-solutions---principles-for-analysing-self--and-co-regulation?v=332518

28 ACMA 2015 *Optimal conditions for effective self- and co-regulatory arrangements* https://www.acma.gov.au/sites/default/files/2019-08/Optimal%20conditions%20for%20effective%20self%20and%20co%20regulatory%20.pdf

29 The factors included direct benefits to the industry, reputational sensitivity, moderate degrees of conflict between public and private interests, transparency, and accountability.

30 Karen Lee 2018 *The Legitimacy and Responsiveness of Industry Rule-making* Hart Publishing

31 Karen Lee, Derek Wilding, Kieran Lindsay & Vidya Kathirgamalingam 2024 *The Enforcement of Telecommunications Consumer Protections* https://www.uts.edu.au/sites/default/files/2024-04/COPY%20CMT%20Enforcement%20Report%202024_0.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,[1] a simple way to ensure that Codes are consistent with the 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.

1 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 (*https://www.infrastructure.gov.au/sites/default/files/documents/amending-the-online-safety-basic-online-safety-expectations-determination-2022-consultation-paper-november2023.pdf*)

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*[2] (**the amending instrument**) with effect from effect from 31 May 2024.

2 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*)

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[3] 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):

> 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.

3 Minister for Communications 2024, Online Safety (Basic Online Safety Expectations) Amendment Determination 2024, pages 7-9 (*https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-bose-amendment-determination-2024.pdf*)

...

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.[4]

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

(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.

4 Office of the 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*)

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;[5] 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.

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.

5 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*)

4.6 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'.[6] 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,[7] the lack of any requirement under the Code 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.

6 Instagram 2024, Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents (*https://about.instagram.com/blog/announcements/instagram-teen-accounts*)

7 Office of the eSafety Commissioner, State of Play - Youth, Kids and Digital Dangers (3 May 2018) page 20-21 (*https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf*)

Does digital co-regulation function in children's best interests?

October 2024

POLICY BRIEFING

https://au.reset.tech/

Reset·Tech AUSTRALIA