How outdated approaches to regulation harm children and young people

and why Australia urgently needs to pivot

Dr Rys Farthing
Reset Australia & ChildFund Australia
Dec 2022

Executive Summary

Australia should be the safest place in the world to go online, but it is not. Australia's reliance on self- and co-regulation has played a big part in this failure. 'Co-regulation' allows industry to write their own rules and guidelines — self-regulation in all but name — and has consistently failed Australians.

This is a live policy debate. Co-regulatory frameworks are currently being developed for children's online safety and could see Australia continue to fail children online. The report documents that:

1. **Co-regulation does not meet community expectations**, and the public overwhelmingly wants regulation drafted by regulators or legislators. A poll of adults found that only 21% trusted the social media industry to write their own codes, and the majority said they would prefer if independent regulators drafted any safety and privacy codes. Likewise, only 14% of teenagers polled said they trusted social media companies to 'write the rules'.

2. **Co-regulation demonstrably leads to weaker protections**. Exploring the draft online safety codes written by industry for Australia to similar codes written by regulators elsewhere in the world, it becomes apparent that co-regulation offers weaker protection. We document three examples:

    - Young people's accounts must be set to "maximum privacy" up until the age of 18 according to regulator drafted Codes, but only up until the age of 16 according to the proposed industry drafted Codes for Australia. This leaves Australian 16 & 17 year olds less protected
    - Children's precise location data could still be collected in Australia according to the proposed industry-drafted Code, creating real safety and privacy risks. Regulator-drafted Codes elsewhere in the world prevent the collection of unnecessary children's location data
    - Child sexual abuse reporting requirements could be higher in the industry-drafted Code than legislator drafted protections in the UK.

3. **Co-regulation is inappropriate given the level of risk technology creates**, and the behaviour of dominant Big Tech firms. Technology creates significant risks for the Australian community, including public health risks, and there is a track record of 'undermining' emerging regulations among the tech sector.

It recommends that the reliance on co-regulation for the technology sector be replaced by the introduction of proper, regulator-drafted regulation.

The three main approaches to industry regulation:

- **Self-regulation** - industry representatives write and oversee their own rules
- **Co-regulation** - industry representatives write and oversee their own rules, but government provides legislative backing to enable these rules to be enforced by regulators
- **'Proper' regulation** – explicit regulation written and overseen by regulators or legislators, often called black letter law.

Contents

Outdated approaches to regulation harm Australians online

AUSTRALIA SHOULD BE THE SAFEST PLACE IN THE WORLD TO GO ONLINE, BUT IT IS NOT. AUSTRALIA'S RELIANCE ON SELF AND CO-REGULATION PLAY A BIG PART IN THIS FAILURE

In many ways, Australia has been at the vanguard of tech regulation. We passed the world's first Online Safety Act, had the world's first eSafety Commissioner and drafted the initial News Media Bargaining Code; we developed legislative frameworks that other countries have since sought to emulate. But the capacity of Australia's policy framework to generate much needed change is consistently hampered by the 'light touch' ways our legislative frameworks become industry regulation.

An anachronism from the '90s means that much tech regulation is developed through 'co-regulatory' processes, allowing Big Tech to write their own guidelines and rules about how to implement legislation. This approach — self regulation in all but name —has consistently failed Australians. Co-regulation has seen the groundbreaking legislation passed in Australia ultimately hamstrung at the point of implementation.

This is a live policy debate, with consequences for Australians here and now. As the new Albanese Government wrestles with some of the most important questions in digital regulation, such as how to effectively update our privacy laws, how to meaningfully protect consumers and correct profound market imbalances, and how to enhance our online safety regulations so that they proactively address the full breadth of harms children and families face, co-regulation has the capacity to neutralise each of these efforts.

For example, co-regulatory codes are 'on the table' for the next phase of implementing the Online Safety Act. As section 2 of this report outlines, weak safety codes have already been drafted by industry. Further, as the Attorney General considered how to progress on privacy enhancements, co-regulatory codes could also be considered. As this report documents, these critical policy initiatives could fail because of co-regulation. Moving towards proper regulation is a simple policy pivot, but has the capacity to demonstrably improve the digital landscape for all Australians.

The three main approaches to industry regulation:

- **Self-regulation** - industry representatives write and oversee their own rules
- **Co-regulation** - industry representatives write and oversee their own rules, but government provides legislative backing to enable these rules to be enforced by regulators
- **'Proper' regulation** – explicit regulation written and overseen by regulators or legislators, often called black letter law.

This research documents the failures of co-regulation. It demonstrates that:

1. Co-regulation does not meet legitimate community expectations, and the public overwhelmingly wants regulation drafted by regulators or legislators
2. Co-regulation demonstrably leads to weaker protections, using a case study around online safety codes
3. Co-regulation is inappropriate given the level of risk technology creates, and the behaviour of dominant Big Tech firms

Technology companies should not be able to write and mark their own homework, and the time has come for proper regulation, drafted by regulators or legislators.

1. Co-regulation does not meet legitimate community expectations

Co-regulation does not meet legitimate community expectations, and the public overwhelmingly wants regulation drafted by regulators or legislators. In Dec 2022, YouGov polled 1,508 Australians to explore their trust in co-regulation.

Trust in social media companies as code authors was lacking. **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).

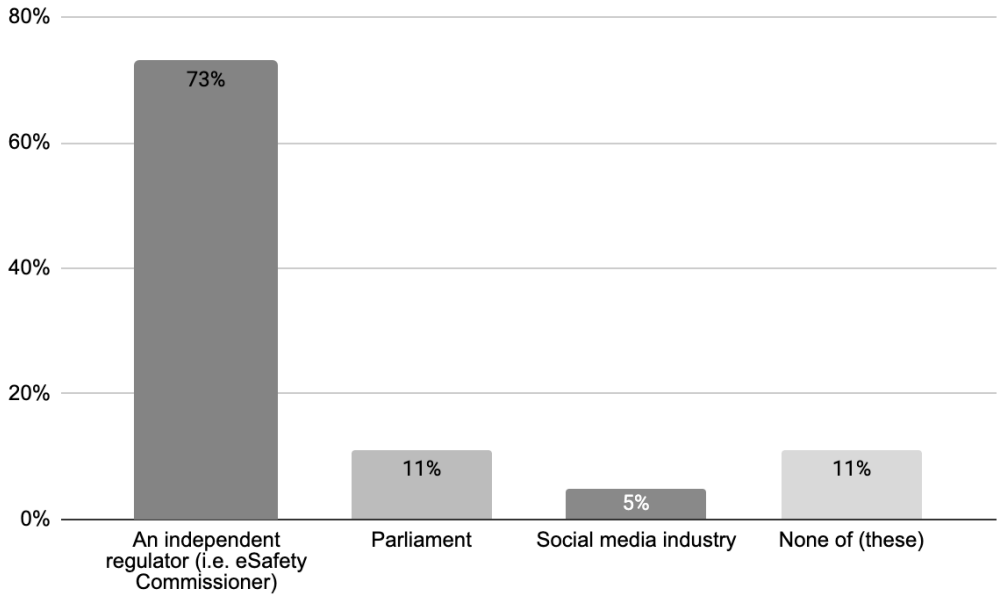

Figure 1: People's preference about who should write the codes for online safety for children (n=1,508) [If you had to choose, who would you most prefer to write the codes about online safety for children?]

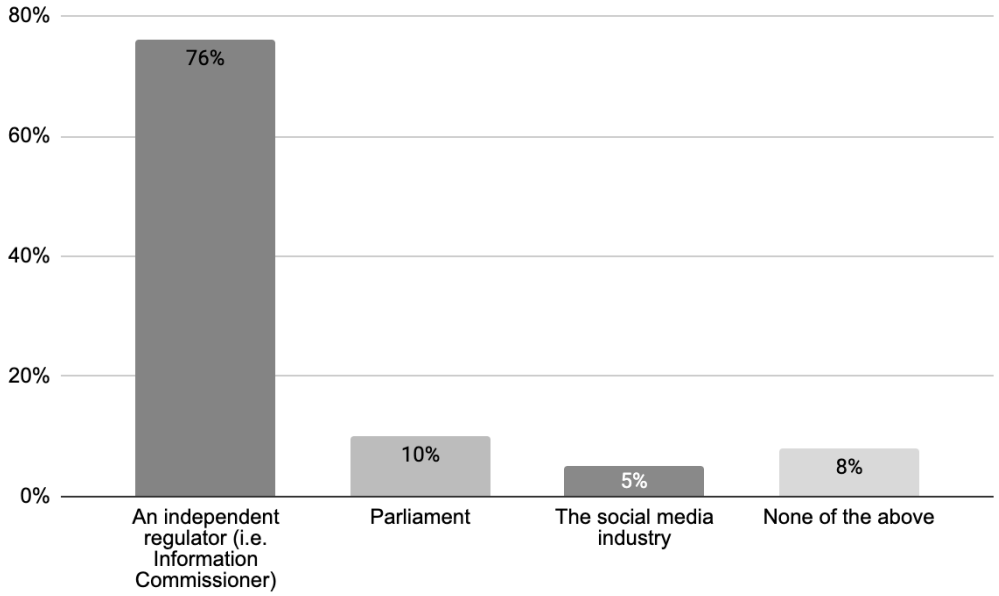

Figure 3: People's preference about who should write the codes for privacy safety for children (n=1,508) [If you had to choose, who would you most prefer to write the codes about online privacy for children?]

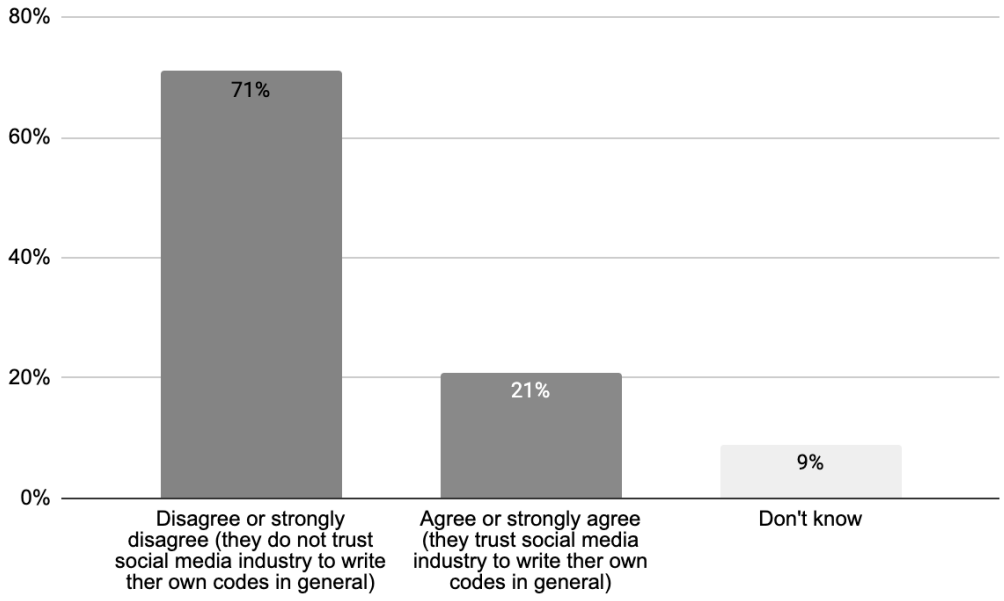

Figure 3: People's response to the statement 'I trust the social media industry to write their own codes about online privacy and data protection in general' (n=1,508).

Given that a number of proposed co-regulatory frameworks affect children and young people, in April 2022, YouGov polled 506 16 & 17 year olds from around the country asking for their thoughts about co-regulation around 'privacy rules'.

Only 14% of young people polled said they would trust social media companies to write the rules about how to keep their data safe and private (see figure 4). We asked who they thought should write the rules, and **73% said they thought either regulators or legislators should draft the rules** (see figure 5).

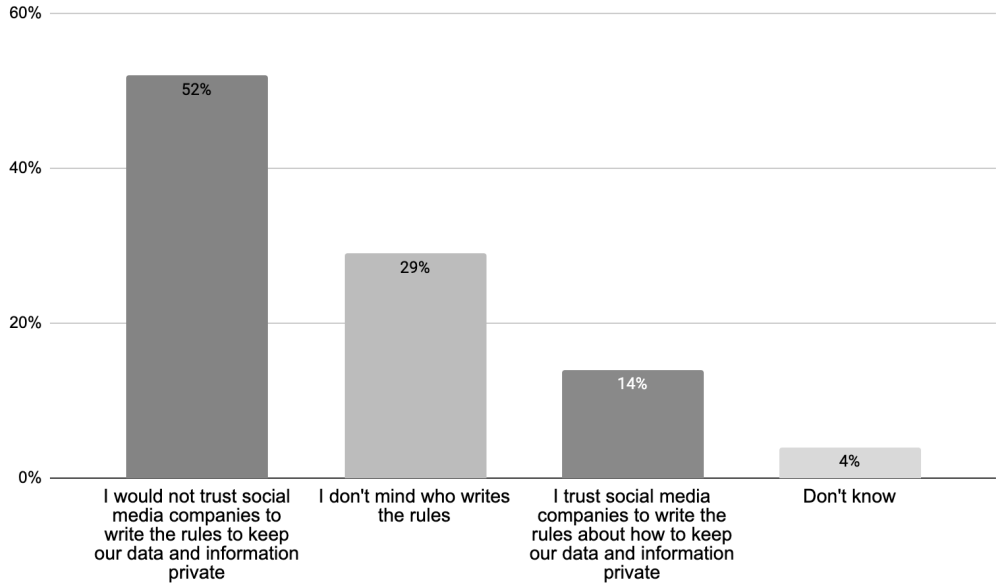

Figure 4: Young people's response to the prompt 'The Government is proposing that social media platforms themselves should write the (rules about how to keep Australians data and information privacy)' (n=506)

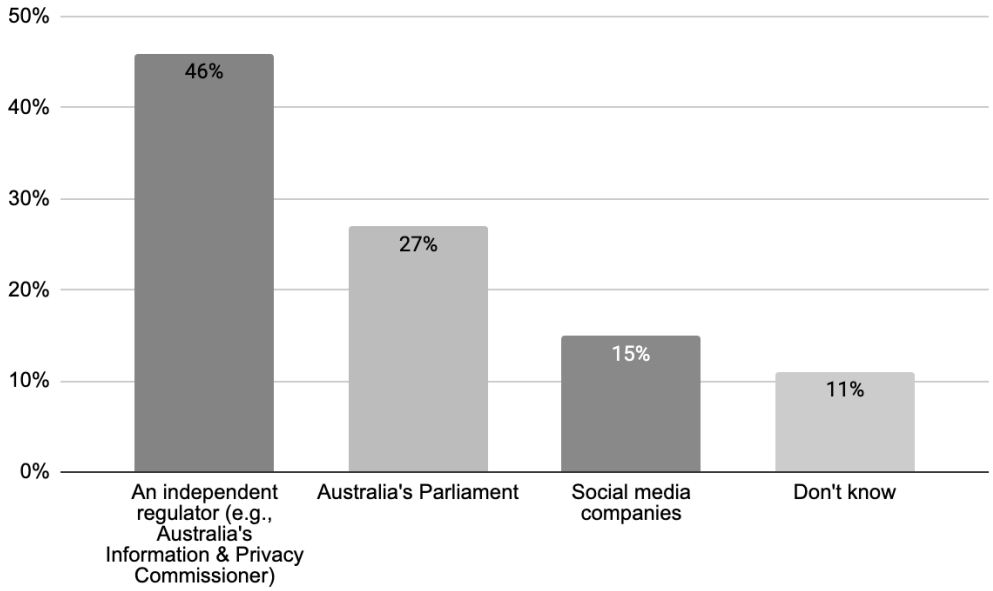

Figure 5: Young people's response 'If you had to choose, who do you think would write the rules to protect information and data privacy for young people?' (n=506)

2. Co-regulation demonstrably leads to weaker protections

3 WAYS CO-REGULATION HAS FAILED CHILDREN

In September 2022, a number of industry drafted Online Safety Codes were released for public consultation.[1] These Codes were drafted by six industry groups,[2] ranging from those representing social media companies, gaming to telecoms.

Comparing these industry drafted Codes with regulator drafted that address similar issues in other jurisdictions, the weakness of co-regulation becomes apparent. Australia's Online Safety Codes propose weaker standards of care than exist elsewhere in the world. We explore three simple examples, comparing the proposed industry-drafted Online Safety Code in Australia with three Codes drafted by regulators and legislators; the UK's *Age Appropriate Design Code* (UK 2020), Ireland's *Fundamentals for a Child Oriented Approach to Data Processing* (Ireland 2021), and California's *Age Appropriate Design Code* (California 2022).

The proposed final versions of these Codes should now be with the Office of the eSafety Commissioner for consideration, but are not publicly available. For brevity, the discussion below highlights three examples of demonstrable weaknesses in the draft Codes vis-a-vis regulator drafted Codes, which we believe still exist in the final version.[3]

1. AGE AT WHICH CHILDREN'S ACCOUNTS DEFAULT TO PRIVATE

Every time a young person creates a new account on a platform which has 'profiles', 'accounts' or 'handles', that company has a choice. The default settings for that child's account can be set to the most private, maximising their privacy and security, or they can 'default' to public, maximising engagement and visibility and profit for the company. It is a stark choice. Children's best interests are better served with private accounts that maximise safety and privacy; whereas commercial interests are better served with public accounts that maximise engagement. Young people can, of course, change these settings but everytime a child opens an account, a company has an opportunity to nudge them towards privacy and safety, or not.

These nudges are important for children's privacy and safety. Meta themselves have outlined the value of private accounts, stating:

---

[1] Australia's co-regulatory Online Safety Codes were prepared in accordance with the *Online Safety Act* 2021 (Cth), which lays out expectations that industry bodies will develop a range of Codes associated with the Online Safety Scheme. This includes Codes that describe procedures for dealing with "Class 1 materials" (illegal materials, such as child sexual abuse material, and pro-terror material) and/or Class 2 Materials (such as X-rated pornographic materials).

[2] Including Communications Alliance (CA), Digital Industry Group Inc. (DIGI) Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance (BSA), Interactive Games and Entertainment Association (IGEA) and Consumer Electronics Suppliers' Association (CESA).

[3] Reset and others raising these three issues with the industry drafters through a required consultation process. The industry drafters stated that "in response to feedback, the Code provisions concerning privacy settings on children's accounts have been amended to apply to children under 16", for example. This suggests these three issues persist in the final version currently under consideration, alongside many others (see here)

> *"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."*[4]

Accordingly, the proposed Online Safety Codes include proposals about defaulting children's accounts to private. They propose a 'minimum age' under which children's accounts must default to public, and at what age young people's accounts can default to public. When we compare the minimum ages proposed by industry draft Codes compared to regulator drafted Codes, we can see that the industry drafted proposals leave Australian 16 and 17 year olds unprotected.

AGE UNDER WHICH YOUNG PEOPLE'S ACCOUNTS MUST 'DEFAULT TO PRIVATE'[5]			
	Who 'wrote' the rules?	**On social media**	**On online games**
UK	Regulators/ legislators[6]	18	18
Ireland	Regulators	18	18
California	Legislators	18	18
Australia	Industry	16[7]	16

This should not be understood as a one-off accident. International experimental research has demonstrated that in jurisdictions where regulators and legislators have written the rules, 16 and 17 year olds are routinely protected, but where rules written by regulators and legislators do not exist, teenagers are unprotected[8] (See Appendix 1).

Indeed, some social media platforms themselves have made clear that this is a deliberate choice. Newly published documents leaked from the whistleblower Francis Haugen suggest that Meta have carefully considered and limited this trade off. A document called '*Should we default teens into privacy settings'* ultimately recommends against defaulting to private settings because 'data projections show a strong

[4] Meta 2021 'Giving young people a safer, more private experience on Instagram' [link]
[5] Meaning they must be set to a private account, or otherwise the have the highest privacy settings turned on in default mode
[6] The UK's *Age Appropriate Design Code* was written by the regulator (the ICO) and subsequently passed by parliament
[7] According to the draft Code for Social Media services made available, they must "have default settings that are designed to prevent (children) from unwanted contact from (strangers), including settings which prevent the location of the child being shared with other accounts by default", but there is no specific mention of defaulting children's accounts to private. The response from the industry drafters to this point was to confirm that it would be 16 [link]
[8] See Fairplay 2022 *Discrimination by Design* [link]

potential for loss of valuable interactions in DMs (direct messages)'.[9] When Meta finally introduced a minimum age under which they would default young people's accounts to private, in anticipation of the UK's Age Appropriate Design Code in 2020, they announced:

> *"starting this week, everyone who is under 16 years old (or under 18 in certain countries) will be defaulted into a private account when they join Instagram".*[10]

Australian teenagers will be less protected than teenagers in "certain countries" because we allow industry to draft their own rules.

2. COLLECTING CHILDREN'S PRECISE GEOGRAPHIC LOCATION DATA

Many digital services and products collect people's geographic location details, even when it is not necessary to provide the service. The majority of Australians find this unacceptable; the OAIC's survey into community attitudes to privacy found that two-thirds (62%) of Australians were uncomfortable with digital platforms and online businesses tracking their location through their mobile or web browser.[11] Despite this, location details are routinely collected and widely shared by companies.[12] This includes children and young people's location data. For example, EdTech products commonly used in Australian classroom's collect location data, including; Zoom, Microsoft Teams and Cisco WebEx.[13]

Children's location data is extremely sensitive and inappropriate disclosure can create safety risks. Accordingly, the proposed Online Safety Codes include proposals about how to handle children and young people's precise geographic location. Again, when we compare the safety measures proposed by industry draft Codes compared to regulator drafted Codes, we can see that the industry drafted proposals are significantly weaker.

In Australia, the proposal is to not *broadcast* children's location. In jurisdictions where codes have been drafted by regulators and legislators, they propose the stronger step of not *collecting* children's locations in the first instance. Preventing services from broadcasting precise locations is a significantly weaker step than preventing them collecting location data, because it overlooks the risks presented from:

- Data security flaws. Collecting troves of location data creates inevitable security risks from malicious hacking to a lack of internal controls about which staff, if any, should be able to access children's GPS locations. The scale of the recent Optus[14] and Medicare[15] breaches, and the gravity of the harms enabled by now-convicted abuser Alexander Jones' ongoing access to the Victorian DHSS' vulnerable children's database[16] suggest that these are not 'pedantic' considerations. Security issues can affect many children and cause immense harm.

---

[9] Instagram UX Research nd *Should we default teens into privacy settings* [link]
[10] Meta 2021 'Giving young people a safer, more private experience on Instagram' [link]
[11] OAIC 2020 *2020 Australian Community Attitudes to Privacy Survey* [link]
[12] For example, location data is un-selectively broadcast in the 'Real Time Bidding' process that drives our personalise advertising feeds. Each American has their location data broadcast 747 times per day to potential advertisers, and in Europe, where data collection is more stringently regulated, 376 times a day.
[13] Human Right Watch 2022 *How Dare They Peep Into my Private Life?* [link]
[14] David Spears 2022, 'Federal government to unveil new security measures following massive Optus data breach' *ABC News* [link]
[15] See Sashwat Awasthi & Lewis Jackson 2022 'Australia's Medibank says data of 4 mln customers accessed by hacker' *Reuters* [link]
[16] Sarah Curnow & Josie Taylor 2021 'About a boy' *ABC News* [link]

- Errors and missteps from services. For example, a simple failure of process saw Instagram make children's contact details publicly available if they simply opened business accounts.[17] Children's precise location data is not immune to failures of process, even if digital services agree in principle to not broadcast locations, mistakes happen.

- Commercial harm arising from this data. Not *broadcasting* GPS data does not prevent online service providers using and selling this data for commercial exploitation, such as targeted advertising. We note again, that while Europe is moving to ban targeted advertising to children, this Code appears to have been drafted in ways that deliberately enable this ongoing practice in Australia. Again, this is out of step with emerging global protections.

PROTECTIONS FOR CHILDREN'S PRECISE LOCATION (GPS LOCATION)			
	Who 'wrote' the rules?	**On social media**	**On online games**
UK	Regulators/ legislators	Must not collect by default	Must not collect by default
Ireland	Regulators	Must not collect by default	Must not collect by default
California	Legislators	Must not collect by default	Must not collect by default
Australia	Industry	Must not broadcast by default	Must not broadcast by default

Australian children's precise location data will continue to be collected at scale and pose safety risks, because we allow industry to draft their own rules.

3. CHILD SEXUAL EXPLOITATION & ABUSE MATERIAL REPORTING REQUIREMENTS

When child sexual abuse is suspected, it should be reported to the relevant authorities. Indeed laws in Queensland, Tasmania, the Northern Territory, Victoria and New South Wales require this, with other states requiring this for certain professions like teachers and doctors.[18]

This requirement isn't fully translated into the industry drafted codes. For example, compliance measure 1 in the Social Media Services Code suggests that:

> *If a provider of a social media service:*
> a. *identifies CSEM (Child Sexual Exploitation Material) and/or pro-terror materials on its service;* ***and***
> b. *forms a good faith belief that the CSEM or pro-terror material is evidence of serious and immediate threat to the life or physical health or safety of an Australian adult or child (i.e. an adult or child ordinarily resident in Australia)*

[17] Natasha Lomas 2022 'Instagram fined €405M in EU over children's privacy' *Techcrunch* [link]

[18] In Queensland *(Criminal Code (Child Sexual Offences Reform) and Other Legislation Amendment Act 2020*), Victoria (*Crimes Amendment (Protection of Children) Act 2014)*, Tasmania (*Criminal Code Act 1924, Sec 105A*), New South Wales (*Crimes Act 1900, Sec 316A*) and the Northern Territory (*Care and Protection of Children Act 2007*) it is an offence for any adult not to report sexual offending, or suspected offending, against children. In WA & SA, certain mandated professionals, employees or volunteers who work within certain mandated organisations are legally bound to report sexual offending, or suspected offending, against children.

> *It must report such material to an appropriate entity within 24 hours or as soon as reasonably practicable.*[19]

All images of child sexual exploitation should raise suspicions that abuse is or has occurred. Yet industry has added an 'and', and a second higher threshold, in reporting requirements. Any social media company must also form a belief that the child abuse material represents an immediate threat to a child before they report it. This potentially provides social media companies discretion to decide which images represent a serious and immediate threat to a child and which do not, and which to report and which not to. This discretion may be problematic. Reporting all CSEM materials to authorities may share useful evidence or allow authorities to uncover patterns of behaviour and threats unknown to staff at Meta or Snapchat. As the Australian Federal Police explain "There is no information too small or insignificant. Something that may appear small or insignificant could prove vital to a police investigation."[20]

This proposal is weaker than other reporting standards, which have been drafted by legislators. For example, the UK's draft *Online Safety Act* requires all child sexual exploitation and abuse content to be reported when it is detected, with detection defined as simply "when a provider becomes aware of the content", without space for interpretation about threat levels.[21]

Vulnerable Australian children, who are depicted in child sexual exploitation material, may be less comprehensively protected because we allow industry to draft their own rules.

[19] Emphasis added. See *Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material) Public Comment Version 01/09/2022* [link]
[20] The AFP's Australian Centre to Counter Child Exploitation (ACCE) 2022 *Report Abuse* [link]
[21] UK 2022 *Online Safety Act (Bill)* Sec 63(4)

3. Co-regulation does not adequately address the risks posed

In 2007 and 2010, the Australian Government released a *Best Practice Regulation Handbook*[22] that outlined criteria and considerations to help policy makers assess which level of regulation was most appropriate for industry and issue. Like co-regulation itself, the handbook is now out-of-date but it provides some insight into the thinking at the time about the limits of self- and co-regulation, and presents some criteria for consideration in assessing when proper regulation might be better suited. The risks posed by technology have all of the characteristics of a policy problem warranting proper regulation, drafted by regulators and legislators.[23]

The Best Practice Regulation handbook notes that self-regulation is a feasible option only 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 (could) be fixed by the market itself"*

Conversely, it notes that government regulation should be considered where:

- *"The problem is high-risk, of high impact or significance; for example, a major public health and safety issue*
- *The community requires the certainty provided by legal sanctions*
- *Universal application is required ...or*
- *There is a systemic compliance problem with a history of intractable disputes & repeated or flagrant breaches of fair trading principles, & no possibility of effective sanctions being applied"*

The threshold warranting proper regulation has been exceeded, when reflecting on these considerations. As we saw during the pandemic, Australia's weak self-regulatory code on mis and disinformation on social media enabled significant public health and safety concerns.[24] Likewise, the community expects the certainty of legal standards. As the YouGov polling above notes, Australians appear to expect proper regulation around these issues. The problem's cannot be fixed by the market themselves; the Digital Platforms Inquiry powerfully highlighted the significant market imbalance benefiting Big Tech,[25] that requires government intervention to correct.

There is also a demonstrable issue of systemic noncompliance among tech companies when it comes to engaging with emerging regulations. From Facebook's appalling attempt to undermine the News Media

[22] Australian Government 2010 *Best Practice Regulation Handbook* Canberra
[23] For a more detailed analysis, see Dhakshayini Sooriyakumaran & Rys Farthing 2020 'Why the Era of Big Tech Self-Regulation Must End' *AQ Magazine* [link]
[24] For example, on Facebook we saw the rapid increase in membership to and engagement with groups peddling 'anti-vaxx' and vaccine hesitant content in Australia (Reset Tech Australia 2021 *Anti-vaccination & vaccine hesitant narratives intensify in Australian Facebook Groups*) [link]
[25] ACCC 2019 *Digital Platforms Inquiry* [link]

Bargaining Code's development[26] (which they are repeating in Canada[27] and the US),[28] Google's fine for negotiating in bad faith around France's News Media Code,[29] to Google's alleged attempt to collude with Apple, Facebook and Microsoft to stall the implementation of children's privacy regulation in the USA,[30] this does not appear to be an industry inclined to join the table and draft robust regulation within the spirit of the law.

But once strong codes and regulations are in place, technology companies are obliged to comply.[31]

[26] Where documents suggest that they deliberately wreaked havoc in implementing a temporary news blackout (See Keach Hagey, Mike Cherney & Jeff Horwitz 2022 'Facebook Deliberately Caused Havoc in Australia to Influence New Law, Whistleblowers Say' *Wall Street Journal* [link]

[27] As Canada seeks to implement their own News Media Bargaining Code, Facebook are repeating their poor behaviour (See Ishmail Shakil 'Facebook threatens to block news content over Canada's revenue-sharing bill' *Reuters* [link])

[28] Similar threats are being made in the US. (See Brian Fung 2022 'Meta threatens to remove news content over US journalism bargaining bill' *CNN*[link])

[29] Ian Campbell 2021 'Google fined €500 million in France over bad faith negotiations with news outlets' *The Verge* [link]

[30] Leah Nylen 2021 'Google sought fellow tech giants' help in stalling kids' privacy protections, states allege' *Politico* [link]

[31] For example, the implementation of the regulator drafted, legislator passed *Age Appropriate Design Code* 2020 (UK), led to a raft of changes in digital services in the UK, from turning off geolocation tracking to turning off private messaging between children and adult strangers. See ICO 2022 *"Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's code* [link]

Recommendations

To ensure the implementation of *effective* regulation for Big Tech, the new Government should consider pivoting away from co-regulation to regulator and legislator drafted regulations for the industry. This is an opportunity to reset Australia's approach to Big Tech, and deliver meaningful changes in the digital environment Australians use. This would require broad changes across a number of laws, but could be progressively implemented.

In the short term:

1. The Online Safety Codes currently 'in the pipeline' should not be registered, and instead stronger more robust Codes could be drafted by the eSafety Commissioner
2. An in-principle commitment could be made for all new regulations to be written by regulators or legislators

In the medium term:

3. The ongoing review of the *Privacy Act* could specifically address the powers of the Information and Privacy Commissioner to draft codes by default
4. Any privacy codes emerging before the *Privacy Act* is updated should be drafted by the Information and Privacy Commissioner, especially around children's privacy

In the long term:

5. All existing self- and co-regulatory mechanisms in operation, such as the Mis and Disinformation Code, should be gradually replaced with regulator drafted codes. As each code comes up for its scheduled review, instead they should be handed back to the relevant regulator to begin the process of drafting a new code.
6. Relevant regulatory bodies would need to be resourced adequately in order to achieve this.

Appendix

As exploration of default privacy settings for 17 year olds by jurisdiction[32] demonstrates the impact of proper regulation on driving up safety standards for teenagers. In each instance, where regulator or legislator guidance exists or is imminent, protections for 17 year olds are stronger.

HAS REGULATOR / LEGISLATOR DRAFTED RULES?[33]		WHAT HAPPENS WHEN A 17 YEAR OLD OPENS A NEW ACCOUNT ON INSTAGRAM's APP?	WHAT HAPPENS WHEN A 17 YEAR OLD OPENS A NEW ACCOUNT ON TIKTOK's APP?
Australia	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Argentina	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Brazil	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Canada	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Colombia	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Ethiopia	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Ghana	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Indonesia	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
Massachusetts, USA	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
South Africa	❌	Prompts user to choose 'public' or 'private'	Account defaults to public
UK	✅	Account defaults to private	Prompts users to choose 'private' or 'skip'[34]
Slovenia	✅	Account defaults to private	Prompts users to choose 'private' or 'skip'
Germany	✅	Account defaults to private	Prompts users to choose 'private' or 'skip'

With thanks to Dhakshayini Sooriyakumaran for her wisdom with survey design and insights around section 3.

[32] See Fairplay 2022 *Discrimination by Design* [link]
[33] Including well publicised draft and proposed rules, yet to come into force
[34] Skipping this prompt defaults users to public. See Fairplay 2022 *Discrimination by Design* [link]

Reset. AUSTRALIA

au.rest.tech

ChildFund Australia

www.childfund.org.au

AUSTRALIAN CHILD RIGHTS TASKFORCE

www.childrightstaskforce.org.au

More information
hello@au.reset.tech

December, 2022