Reset.
AUSTRALIA

Response to the ACCC Digital Platform Services Inquiry

Interim Report #5

Reset Australia
Feb 2023

Reset.
AUSTRALIA

Contents

1. About Reset Australia & this submission

Reset Australia is an independent, non-partisan policy initiative 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 and strengthen digital markets.

This submission has been prepared in response to the **ACCC Digital Platform Services Inquiry, Interim Report #5**. We provide an overview of Reset's broader thinking about the issues of competition and consumer issues on digital platforms in Australia, as well as responding directly to some of the questions posed in the ACCC's discussion paper.

Specifically, we respond to the ACCC's queries around the nature of type of regulations, designations and obligations that would be needed to reshape the digital landscape for Australians. This includes responses to questions 1, 3, 8, 10, 13, 15, 17, 18, 19, and 20.

2. The need for a comprehensive digital regulatory framework for Australia

Reset Australia welcomes the ACCC's Digital Platform Services Inquiry's Interim Report #5, specifically the focus on describing the need for and potential shape of a new regulatory regime for digital platforms. We recognise that this is part of the ACCC's ongoing commitment to review and implement recommendations from the 2019 Digital Platforms Inquiry, which compellingly documented the need for broader regulatory reforms in Australia.

Reset Australia strongly believes that this comprehensive approach described in the Inquiry and subsequent reports is urgently needed. It must include consumer protection and competition law, privacy laws and online safety regulations to create a digital world that enhances Australian democracy and improves lives.

Reset Australia has previously outlined five directions for future policy to ensure Australia arrives at an effective, coherent tech regulation framework, which inform this submission.[1] We have summarised below.

[1] Reset.Tech Australia *The future of digital regulation in Australia*
https://au.reset.tech/news/the-future-of-digital-regulation-in-australia-five-policy-principles/

2.1 Eliminating risks from systems and processes

Regulation needs to pivot towards targeting risks created across the systems and processes developed by digital services. The aspects of systems and processes, and related risks, that regulation could address includes:

- Algorithms. Including content recommenders systems and ad delivery systems
- Platform design. Including design abuses and dark patterns
- Specific features. Specific features that create risks need to be addressed

It is these sorts of systems and processes that manufacture and amplify risks. However, none of them are inevitable and these risks exist because of choices made by digital platform services. Social media platforms can change and improve their systems, and regulation can incentivise them to do so.

2.2 Expand regulations to address community & societal risks

Existing legislation addresses a collection of individual risks that leave Australians vulnerable to collective risks. Collective risks come in two interconnected forms.

- Community risks, such as those facing indigenous communities, migrant communities, people of colour, women, children and LGBTIQ+ people. These communities often suffer unique and disproportionate harms in the digital world that extend beyond individual risks posed by content. Disinformation and hate speech can affect particular communities in ways that differ from individual harm.
- Societal risks. The scale and reach of social media platforms has the capacity to influence and affect Australian institutions, such as Parliament, the Press and healthcare systems, often with destabilising effects.

Expanding the definitions of harms (and risks) addressed in Australia's regulatory framework would better protect Australian communities and society at large.

2.3 Ensure regulation creates accountability & transparency

There are multiple ways governments can regulate the digital world, but the most effective policies require accountability and transparency from tech platforms themselves. Regulations that identify the core risks as stemming from platforms themselves — and squarely place the burden of responsibility on digital services — should be prioritised.

Regulation can place duties on users in multiple ways, but these are often inappropriate or ineffective:

- Solutions that position individual users (especially children and parents) as key actors in improving safety are often inappropriate and will fail to protect all Australians
- Solutions that pass responsibility on to users (as parents or consumers) to read 'the fine print' or consent to a risky system misrepresents the power asymmetry between users and digital platforms

- Solutions that position individual users (be they 'trolls' or influencers) as the key actors responsible for harm undersells the role of platforms in creating the risky digital environments that enable and encourage toxic actors.

Accountability also requires transparency. Legislators, regulators, researchers and civil society need to have up to date understandings about the specific mechanics of platform's functionalities and outcomes in order to better hold them to account.

2.4 Ensure the regulatory framework is comprehensive

The rapid growth of the technology has seen Australia's issue-by-issue (e.g. 'cyber bullying', 'trolling' etc), sector-by-sector (e.g. 'social media platforms' 'messaging services' etc) regulatory framework struggle to keep pace. Many new and emergent technologies are missed, and innovative companies straddling the gaps between existing industry definitions are inappropriately regulated.

- A service-by-service approach fails to address the vertical integrations and shared functionality of may digital platforms
- An issue-by-issue approach cannot anticipate risks created by innovations and emergent technologies.

These gaps suggest that the current approach is unable to future-proof the regulatory framework, and that as technologies evolve, more and more gaps will emerge. Risk focused, systemic models may be more successful at future proofing themselves.

2.5. Ensure regulation is strong and enforced

Big tech poses big risks and necessitates a robust regulatory response. However, because Australia has to date engaged self- and co-regulatory models by default, our regulatory framework has often failed to reduce risks as rigorously as they otherwise may have.

Future regulation needs to start from the premise that self- and co-regulation will not be sufficient. Reset Australia believes self- and co-regulation have a role to play in the Australian regulatory landscape at large, but that unfortunately the risks posed by the digital environment are:

- High impact, and include significant public health and community safety concerns
- Significant to the community, and the public has an appetite for the certainty of robust regulations
- Unable to be adequately dealt with by lighter touch regulations. Digital platforms have demonstrated a track record of systemic compliance issues, including multiple breaches of existing legislation and a generally anaemic response to self-regulation

This warrants a pivot towards primary and subordinate legislation and regulator drafted Standards for digital platforms.

Alongside strengthening existing regulation, regulators need to be resourced and enabled to enforce this, and joined up in ways that do not reproduce the issue-by-issue approach hampering current legislative remedies.

3. Response to the ACCC's specific questions

Question 1: Relying on existing frameworks is too risky

Do you agree with the ACCC's conclusion that relying only on existing regulatory frameworks would lead to adverse outcomes for Australian consumers and businesses? What are the likely benefits and risks of relying primarily on existing regulatory frameworks?

Existing Australian regulatory frameworks are inadequate, and often fail to protect Australian users and businesses. A range of harms proliferate under the existing framework, as the ACCC paper notes these include; unfair trading practices; scams; fraudulent apps, and fake reviews. We would like to note, however, that these harms extend beyond consumers and businesses, and locate them with a broader context too.

The dominant market power of large platforms creates not only a fundamental market imbalance, but also societal imbalances. The processes that lead to the harms outlined in the ACCC's Interim Report 5—network effects, high 'sunk costs', expansive ecosystems, barriers to switching, high-quality user data—are also the same processes that drive many societal harms. For example, access to high-quality users data, reinforced by vertical integrating product offers, rests on the harm of data exploitation. Likewise, the concerning market practices of dominant platforms, from self-preferencing, to denying interoperability, to withholding access to data, mirror their broader problematic social practices. Meta's willingness to intentionally cause havoc by 'turning off the news' during negotiations around the News Media Bargaining Code[2] was not a unique event. It reflects the willingness of dominant platforms to flex their market power to harm companies, consumers *and* societies. Competition harms do not arise in complete isolation.

The existing regulatory framework has demonstrably not risen to either sets of challenges created by the proliferation of digital platforms, competition nor societal. Relying on these frameworks further perpetuates competition and societal risks. This nexus of competition and social risks is increasingly being addressed in other jurisdictions, notably the EU which passed the aligned Digital Services Act and the Digital Markets Act in 2022, and the UK which is in the process of passing an Online Safety Act after establishing the Digital Markets Authority in 2021.

Without updating our regulatory framework, Australia runs the risk of falling behind in terms of market protections, which could detrimentally contribute to the balkanisation of digital regulations. Given the size of the other markets that have or are moving towards addressing these risks, this could leave Australian business on the 'wrong side' of the regulatory fault lines.

[2] Keach Hagey, Mike Cherney & Jeff Horwitz 2022 'Facebook Deliberately Caused Havoc in Australia to Influence New Law, Whistleblowers Say' *Wall Street Journal*

Updating Australia's regulatory framework is essential to safeguard our markets and consumers. This requires both new regulations, including those proposed by the ACCC's Interim Report #5, but also updating other aspects of our regulatory framework, including:

- **Privacy protections**. The unfair use of users data in itself represents a harm to consumers, but also drives unfair market advantages to large, vertically integrated companies that are able to effectively exploit it. Current privacy regulations are unable to prevent this, particularly given the broad failure to protect metadata and 'look-a-like' data, two main datasets held by digital platforms, as personal information.

- **Online safety protections**. Mechanisms to protect vulnerable consumers online are too limited, and mandatory responses—in the form of 'take down notices'—only required once a harm has occurred. Preventive measures, such as Codes addressing systemic safety factors are either voluntary and ineffective (such as the Mis- and Dis-information Code) or co-regulatory and drafted by those currently benefiting from unfair market dominance (such as the Online Safety Codes) and will be inadequate to shift existing business practices. This leaves vulnerable consumers open to excessive harm, and this in itself is a discriminatory and unfair consequence of Australia's existing regulatory framework.

- **Protections for news publishers**. The News Media Bargaining Code (NMBC) has further entrenched unfair power imbalances between news publishers and platforms, with 'voluntary' deals struck at the whim of platforms. This in effect turns any payments made into 'hush money', and disincentives news publishers from challenging platforms. (Either because they have a deal and want to keep it that way, or they are hoping to strike a deal so they want to remain 'friends').[3]

Improving the regulatory framework from a competition perspective will help to remedy some of these harms, and contribute to a broader context of reducing the risks Australians face in the digital world.

Question 3: Alternative regulatory options

Are there alternative regulatory or non-regulatory options that may be better suited?

Mandatory, 'black letter laws' are the most suitable solutions to the risks that Australians face. This includes regulator-drafted Standards and principle and secondary legislation.

Voluntary, self-regulatory Codes have failed to improve standards. The digital platforms market is now a mature market. Facebook, for example, is now 19 years old. Over this time, industry has had ample opportunity to improve its own practices and work collectively to adopt best practice models. This is not what we have seen from the sector. As the ACCC's Digital Platforms Inquiry, and successive interim reports around this, have documented, the market is instead riddled with practices that systemically generate harm to consumers and businesses, from self-preferencing to restrictions on consumer's autonomy, and we would add monopolistic practices.

[3] Reset.Tech Australia 2022 *News Media Bargaining Code: Missed Opportunities* https://au.reset.tech/news/australia-s-news-media-bargaining-code-missed-opportunities/

Take for example, the ineffectiveness of the voluntary self-regulatory code on Mis and Disinformation on Social Media, which has potentially significant consequences for Australian consumers. For example, during the pandemic, while the Code was in force, on platforms that were voluntary signatories we saw the rapid increase in membership to and engagement with groups peddling 'anti-vaxx' and vaccine hesitant content in Australia.[4]

Likewise, co-regulatory Codes that allow industry to in effect set their own rules, also appear ineffective. Take for example, the co-regulatory Online Safety Codes developed by industry representatives towards the end of 2022. Comparing the provisions in these industry drafted Codes, with existing standards and international best-practice demonstrates how these codes fail to drive up practice. For example;

- According to the co-regulatory codes, international best practice dictates that young people's accounts must be set to "maximum privacy" up until the age of 18 (jn the EU, UK and California), but only up until the age of 16 according to Australia's co-regulatory codes. This leaves Australian 16 & 17 year olds less protected because our regulatory framework rests on co-regulation
- Children's precise location data could still be collected in Australia according to our co-regulatory Code, creating real safety and privacy risks. International best practice prevents the collection of unnecessary children's location data in the first instance. Again, this highlights the failure of co-regulation to drive up standards.
- Child sexual abuse reporting requirements appear to be lower than existing Australia child safeguarding standards in Queensland, Tasmania, the Northern Territory, Victoria and New South Wales. This means that leniency of co-regulation has been exploited to set lower standards than existing legal requirements.[5]

This is not a sector that has a strong innate orientation towards embracing effective self- or co-regulatory measures. In fact, the behavior of dominant market platforms suggests that they often do not act in good faith when it comes to any sort of regulatory framework. From Facebook's appalling attempt to undermine the News Media Bargaining Code's development[6] (which they are repeating in Canada[7] and the US),[8] Google's fine for negotiating in bad faith around France's News Media Code,[9] to Google's alleged attempt to collude with Apple, Facebook and Microsoft to stall the implementation of children's privacy

---

[4] Reset.Tech Australia 2021 *Anti-vaccination & vaccine hesitant narratives intensify in Australian Facebook Groups* https://au.reset.tech/uploads/resetaustralia_social-listening_report_100521-1.pdf

[5] Reset.Tech Australia 2022 *Coregulation and Children report* https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/

[6] 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* https://www.wsj.com/articles/facebook-deliberately-caused-havoc-in-australia-to-influence-new-law-whistleblowers-say-11651768302

[7] 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* https://www.reuters.com/business/media-telecom/facebook-threatens-block-news-content-over-canadas-revenue-sharing-bill-2022-10-22/

[8] Similar threats are being made in the US. (See Brian Fung 2022 'Meta threatens to remove news content over US journalism bargaining bill' *CNN* https://edition.cnn.com/2022/12/05/tech/meta-news-content/index.html

[9] Ian Campbell 2021 'Google fined €500 million in France over bad faith negotiations with news outlets' *The Verge* https://www.theverge.com/2021/7/13/22575647/google-fine-500-million-french-authorities-news-showcase

regulation in the USA —[10] evidently, this is not an industry inclined to join the table and draft robust regulation within the spirit of the law. Non-regulatory options simply will not work.

To be effective, responses need to be legislator- or regulator-designed, and as discussed in question 18, mandatory.

Question 8: Scams, apps, fake reviews, and the advertising problem

Do you agree with the ACCC recommendation to introduce targeted measures on digital platforms to prevent and remove scams, harmful apps and fake reviews? Are there any other harms that should be covered by targeted consumer measures, for example, consumer harms related to the online ticket reselling market for live events?

The ACCC's focus on preventing and removing scams, harmful apps, and fake reviews is a step in the right direction. Scams, harmful apps, and fake reviews are excellent examples of the consumer harms on digital platforms. We encourage the ACCC to continue to appreciate that these are harms endured from the relatively unsupervised digital advertising market, a significant profit driver for large digital platforms operating in Australia.

The ACCC has a sophisticated position on digital advertising, having led the *Digital Advertising Services Inquiry*. This inquiry was an appropriate assessment of the business-to-business market dynamics at the time. Since then, our understanding of how digital advertising business models cause consumer harm across the internet has dramatically increased. We direct the ACCC to one of the leading contemporary conceptual frameworks, authored by Tim Hwang.[11] Hwang takes a maximalist assessment of digital advertising as something that not only incentivises online content, but forms the underlying economics of the web.

We encourage the ACCC to revisit the digital advertising ecosystem, not merely as a site for business-to-business harms, but as a vast underbelly of the web requiring more regulatory oversight. The majority of consumer harms from digital platforms that concern the ACCC - the aforementioned issues for this report, and many more, such as personalised pricing and disinformation - stem from a world where advertising is not simply a business service but a central tenet of digital real estate.

One path for the ACCC here is enacting inspection and audit powers over digital advertising transactions, including purchases of ads on social media platforms. Inspection and audit powers are typical features of other industrial regulators in Australia. We note proposals for a safety commissioner in the artificial intelligence domain based on existing models from gene

[10] Leah Nylen 2021 'Google sought fellow tech giants' help in stalling kids' privacy protections, states allege' *Politico* [link]
[11] See *The Sub-prime Attention Crisis* (2020) and *The Theory of Peak Advertising and the Future of the Web* (2013)

technology, food safety, and therapeutic goods.[12] We note that the scope of such a commissioner could sensibly include digital advertising and its associated algorithmic systems. We refer the Committee to our partners in the UK, who have advised numerous regulators on realistic routes to algorithmic inspection.[13]

It is important to consider these regulatory model proposals in the context of live developments in Big Tech transparency efforts. The recent changes around Twitter's API policy proves an alarming point that Big Tech has full flexibility to change course on data access with little warning. We cannot continue to operate under a model where states handle massive information security issues by relying on the invitation or acquiescence of platforms to release data on their terms.

Question 10: An independent external ombuds

Is a new independent external ombuds scheme to resolve consumer disputes with platforms warranted? Can any or all of the functions proposed for the new body be performed by an existing body and, if so, which one would be most appropriate?

We welcome the proposal to empower an ombuds to resolve disputes pertaining to digital markets. A well-established ombuds scheme has the potential to address numerous gaps in accountability and redress in digital markets. However, we recommend that the design of a potential scheme should be considered alongside *proactive* measures. It would be insufficient, for example, to rely on an ombuds scheme to serve as the single relief point for consumer harms on digital platforms. The burden to pursue remedies and accountability measures should not lie exclusively with individual consumers. However, a well-resourced digital markets ombuds acting in tandem with a regulator armed with *Digital Services Act*-level enforcement powers would be appealing.

Question 13: Designation is vulnerable to the power of Big Tech

Do you agree with the designation and code of conduct model proposed by the ACCC for the new competition regime? What would be the main implementation challenges for such a regime?

[12] Will Bateman and Julia Powles (2020), *Response to the Human Rights Commissioner's Discussion Paper* https://humanrights.gov.au/sites/default/files/2020-07/julia_powles_and_will_bateman.pdf

[13] See for example, Jenny Brennan (2020) 'Algorithms in social media: realistic routes to regulatory inspection' *Ada Lovelace Institute* https://www.adalovelaceinstitute.org/blog/algorithms-social-media-realistic-routes-to-regulatory-inspection/

We refer to our previous analysis on this topic, compiled in the context of the *News Media Bargaining Code*. We have extracted the core argument below, as we think there are valuable lessons for future models.

One of the most problematic features of the *News Media Bargaining Code* is the discrepancies in coverage between digital platforms and news media businesses. Their requirements for designation are summarised in the table.

Digital Platforms	News Media Businesses
Ministerial (the Treasurer) designation, but must 'take into account': i) if there is a significant bargaining power imbalance ii) whether the group has made a significant contribution to the Australian news industry (through agreements relating to news content including agreements to remunerate for their content)	A corporation may apply to the ACMA and must satisfy the: i) content test (produce core news content) ii) Australian audience test (serves predominantly an Australian audience) iii) professional standards test (satisfies professional editorial standards, includes provisions for ABC and SBS inclusion) iv) revenue test (greater than $150k)

As the Code only applies to parties which meet these criteria, these provisions hold significant influence. How digital platforms are designated changed significantly over the course of the Code's policy development. The requirement for the Minister to additionally consider 'whether the platform has made significant contributions to the Australian news industry' was the result of last-minute negotiations between Facebook (now Meta) and the Government.

The reliance on Ministerial designation, particularly with the additional consideration around platforms' general contributions, weakens the Code. It allows platforms that make deals with some larger news publishers to avoid engaging with all other Australian news publishers (as per the legislation's original intent). This is economically advantageous for Facebook and other platforms, and deprives many news publishers (particularly small to medium sized businesses) of the economic advantages that would have flowed to them.

Tellingly, two years since the Code was passed, no digital platform has been designated.

A key argument has been that the 'threat of designation' alone compelled the platforms to negotiate deals with the majority of news media players. Whether we would have seen the same outcomes via the Code's mediation/arbitration process is unknown. Unfortunately, relying on this 'threat' ultimately contradicts the spirit of and diminishes the policy for three main reasons:

i. It opens up the application of this law to corporate capture and political posturing
ii. It doesn't ensure consistent and equitable application
iii. It provides a mechanism for digital platforms to evade true accountability and rectification of unbalanced bargaining power, by entrenching more power with the platforms

How this could be improved

Removing Government involvement in designation is key to making the Code equitable and consistent. Harmonisation with how news media businesses are registered under the Code (i.e. independent regulatory assessment on the basis of certain 'tests') is the appropriate way forward.

Specified criteria needs to be developed for digital platform designation that results in automatic inclusion onto the Code to mitigate the impact of replying on Ministerial Discretion.

For example, the ACMA with guidance from the ACCC could determine which digital platforms are to be designated on the Code. This determination could take into account a number of tests, such as:

- Bargaining power tests - if there is a significant bargaining power imbalance
- Market penetration tests - if a certain % of the Australian population are active users of the digital platform
- Revenue tests - if the digital platform makes $X within the Australian market each year
- News content tests - if the platform is used to share, distribute or facilitate engagement with covered news content

Question 15: Principles for designation

Do you agree with the proposed principles for designating platforms for the regime?

In the case of the NMBC, we have seen discretionary designation create a worrying context where any monies paid from platforms to news publishers effectively becomes 'hush money'. News publishers are inherently dissuaded from challenging the process or indeed platforms because they are keen to make a deal. In no way does this redress the power imbalance between publishers and platforms.

Designation for future Codes must not be discretionary, and we agree that the ACCC's broadly lays out an effective set of criteria, but believe that these would need to be strengthened to develop a risk-based set of criteria that applied to *all* digital platforms. Specifically;

- **The use of quantitative criteria**, such as the number of monthly active Australian users and the platform's global revenue must be central. As the ACCC report suggests, these

sorts of criteria are widely used in other jurisdictions, such as EU where the Digital Services Act for example, designates additional responsibilities to 'Very Large Online Service Platforms' as defined by those whose monthly user count is 10% or more of the EU population, or in the US where multiple Bills suggest additional requirements for platforms whose monthly user count exceeds 15% of the population. The use of 'user numbers' as a criteria requires careful consideration in the context of vertical integration however. For example, where a company operates multiple small or medium sized platforms they may evade a 'monthly users of a specific platform' criteria, but if they ID-link users data from multiple platforms they may still benefit from unfair access to high-quality user data causing consumer harm. We also note that some platforms may capture a significant market share of vulnerable users, such as under 18 year olds, but not meet a singular Australian threshold. Likewise, the use of revenue criteria, which is also used in the EU, US and Japan also needs some careful consideration. Many of the most harmful companies—from a competition perspective but also from a social perspective—can be small. For example, many digital services that peddle false reviews (with high SEO) are small in revenue, with an outsized effect on consumer choice.

- **The use of qualitative criteria** could supplement these qualitative criteria. Case-by-case consideration about a platform's intermediary position, substantial market power in the provision of the digital platform service, and whether it operates multiple digital platform services could address some of the issues with revenue- or user-based assessments. This could include consideration around the vulnerability of their user base, the 'risks' their business model creates for consumers and businesses and other market concerns. The development of qualitative criteria should consider how to move from quantitative specificity to a fully-considered risk based model.

Ultimately, transparency and accountability need to be written into the designation criteria to allow broader social oversight and challenge to designation criteria.

Question 17: Targets for Codes and Standards

What services should be prioritised when developing a code? What harms should they be targeted on preventing?

While we principally believe that Australia's regulatory framework needs to move towards standards drafted by regulators, all digital platforms need to be covered by regulatory reforms—Standards or Codes—to improve comprehensiveness.

A service-by-service approach creates too many gaps and often allows companies to cherry pick what regulations might apply to them. (For example, the Online Safety Codes allow companies potentially covered by multiple Codes to select which Code they will be covered

by and apply that Code).[14] This approach can fail to adequately address the shared functionalities and integration between digital platforms.

It also creates many unintended gaps in regulatory oversight. For example, Roblox—an online kids game—highlights the sorts of peculiarities that taking a service-by-service approach can lead to. Like a social media service, Roblox allows the creation of personal avatars; facilitates and encourages interaction and communication between users, and; allows users to create and share games for others to play. But it is not a social media service (as defined under the Online Safety Act) because users do not post content *per se* — they 'post' games. (For clarity, Roblox is covered under the *Online Safety Act* as a 'relevant electronic service' because it facilitates messaging and game play between users). At one stage, this very fine nuance meant that Roblox looked set not to be covered by a proposed Enhancing Online Privacy Act. The draft Act had a user based threshold of 2.5mil users for designation, which is improbably large for a children's game.[15]

This would have create an illogical regulatory situation; because Roblox allows users to 'create and share games' rather than 'create and share content', children would have been protected against cyberbullying under the *Online Safety Ac*t, but would not be protected from privacy incursions by the Enhancing Online Privacy Bill, unless almost all Australia's children join the platform, in which case they then may be protected with regulation again. This is not an ideal framework.

While the Enhancing Online Privacy Bill did not reach parliament, it ultimately highlights the concerns of targeting individual companies or services. Regulations covering all digital platforms, with risk-based requirements, are far more effective.

Question 18: Mandatory requirements

Should codes be mandatory or voluntary?

Codes should be mandatory to ensure they raise standards and are effective.

Voluntary measures do not raise standards; there are insufficient incentives for industry to draft voluntary Codes that 'lift the floor' of practice. The drafting process for the (yet to be registered) Online Safety Codes highlight this. Where industry was able to 'voluntarily' decide what safety measures to include in the Codes and what to leave out, we saw the development of a set of Codes with requirements that were notably 'worse' than many existing practices, and were set well below international best practice standards.

---

[14] "Where a single electronic service could fall within the scope of more than one industry code, the relevant industry participant will only be required to comply with one code for that electronic service. The code that will apply in this situation is the code that is most closely aligned with the predominant purpose of the single electronic service'. There are no guidelines or requirements for deciding which is the predominant purpose. CA & Digi 2022 *Head Terms for all Codes* https://onlinesafety.org.au/wp-content/uploads/2022/08/0_Head-Terms-for-PC_Final-1.pdf

[15] Unless 2.5 million Australians logged on making it a 'large online platform' under the proposed Bill, which was improbable. Roblox is a platform used mostly by children (only 30% of their global audience is over 16). There are a total of 3.6m 5-16 year olds in Australia, making the 2.5m threshold for coverage improbable. (see Jessica Clement 2021 *Distribution of Roblox games users worldwide as of September 2020, by age* www.statista.com/statistics/1190869/roblox-games-users-global-distribution-age/)

Voluntary measures are also ineffective. Australia's previous experience with voluntary codes for digital platforms has failed to produce any changes so far. The Mis- and Dis-information Code, a voluntary Code intended to improve Australia's information architecture failed to do so. To date, only 8 platforms have signed up to this Code and it is widely regarded as weak and lacking impact. Notably, only 2 years after the Code was published, the Government has announced their intention to the ACMA powers to register an enforceable industry Code (or make a standard in the Code development process fails).

Voluntary Codes do not improve practices, are not effective, and function simply to delay the development of mandatory Codes. See the experience in EU, where obligations under the self-regulatory *Code of Practice on Disinformation* (2018) were found to be inadequate, and replaced by obligations within the *Digital Services Act*. Harm happens while we wait for self- and co-regulation to fail, and regulator-drafted industry standards should be the norm. We note the *Privacy Act Review*[16] suggests moving in a regulator-drafted direction for a number of Privacy Codes, which is a positive development.

Question 19: Designing and drafting the regime

Who should be responsible for the design of the proposed codes of conduct and obligations?

Co-regulation has demonstrably failed in the online regulation space. As our response to question 3 highlights, the development of the Online Safety Codes showcase the weaknesses of allowing industry to develop their own Codes. Allowing industry to design and draft their own Codes leads to weaker protections.

Further, allowing industry to draft Codes does not meet community expectations. In Dec 2022, working with YouGov, we polled 1,508 Australian adults about their expectations of regulations for digital platforms, specifically when it came to online safety and privacy. Trust in 'social media companies' to design Codes was distinctly lacking. Only 21% of adults suggested they trust the social media industry to write their own codes, with a strong preference for independent regulators design codes (73% preferring the eSafety Commissioner draft the Online Safety Code, and 76% preferring the Information Commissioner draft any potential privacy Codes).[17] Allowing industry to design Codes does not meet legitimate community expectations in the privacy nor safety domain, and there is no evidence to suggest this would be any different when it comes to competition.

More broadly, there is public support for strong regulatory action. In 2021, a Lowy Institute poll found that 90% of Australians think that the influence social media companies have is an important or critical threat to the vital interests of Australia.[18] Likewise, a 2020 poll by the Australian Financial Review in late 2020 found that 77% of Australians felt that BigTech should

[16] Attorney General's Department, (2023) *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
[17] Reset.Tech Australia 2022 *Coregulation and Children report* https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/
[18] Lowy Institute 2021 *Lowy Institute Poll 2021* https://poll.lowyinstitute.org/report/2021/

face stronger Government regulations.[19] The scale and depth of the public's concerns warrants the strongest possible regulatory response.

There are now legitimate community expectations of explicit regulation of digital platforms, with Standards designed by regulators.

Question 20: Designation under the regime

Who should be responsible for selecting or designating platforms to be covered by particular regulatory requirements?

We believe that independent regulators, in this instance the ACCC, should be responsible for designating platforms.

The experience of the News Media Bargaining Code highlights the risks of allowing Ministers to designate platforms. Ministerial designation entrenches a situation where:

- Designation becomes politicised, which can stall or undermine negotiations between news publishers and platforms.
- The main 'opposition' that needs to effectively and individually lobby for deals became the news publishers themselves, which further address power imbalances.
- Digital platforms retain full control over who they strike deals with, creating further market imbalances. The lack of deal between Facebook and SBS highlights this.
- Limited checks and balances in the deal making process, which reduces the effectiveness of the Code in actually improving public interest journalism.[20]

The experience of the Mis- and Dis-information Code, which is voluntary and in effect allows industry to decide who should be covered by the Code suggests that it is not a particularly effective mechanism for digital platforms either. To date, only eight platforms have signed up,[21] with many digital platforms that have known issues of mis and dis-information uncovered. For example BitChute, Odyssey and Telegram are not signatories despite being available in Australia and known vectors of mis and dis-information.[22] Voluntary 'designation' means that platforms that knowingly engage in harmful practices can simply choose to avoid regulation.

---

[19] Paul Smith 2020 'Big tech on the nose as Aussies demand accountability and tougher laws' *Australian Financial Review*
https://www.afr.com/technology/big-tech-on-the-nose-as-aussies-demand-accountability-and-tougher-laws-20201030-p56a93

[20] Reset.Tech Australia 2022 *Australia's News Media Bargaining Code One Year On*
https://au.reset.tech/uploads/australia-s-news-media-bargaining-code-report-updated.pdf

[21] Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter. See ACMA 2022 *Australian Code of Practice for Disinformation and Misinformation*
https://www.acma.gov.au/online-misinformation#:~:text=you%20have%20concerns.-,Australian%20Code%20of%20Practice%20for%20Disinformation%20and%20Misinformation,%2C%20Redbubble%2C%20TikTok%20and%20Twitter.

[22] Mark Scott 2022 'Fringe social media networks sidestep online content rules' *Politico*
https://www.politico.eu/article/fringe-social-media-telegram-extremism-far-right/