Reset.
AUSTRALIA

Response to the ACCC Digital Platform Services Inquiry

Reset Australia
April 2022

Contents

1. About Reset Australia & this submission

Reset Australia is an independent, non-partisan policy think tank 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.

This submission has been prepared in response to the ACCC Digital Platform Services Inquiry. It provides 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 the harms created for Australians in the digital world, and the type of regulatory framework needed to adequately address this. This includes responses to questions 1, 3, 4, 5, 8, 9, 10, 11, 12 and 16.

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

Reset Australia welcomes the ACCC's Digital Platform Services Inquiry's Discussion Paper number five, and the continuing obligation to review and implement recommendations from the inquiry. The inquiry was a landmark initiative, and documented the need for comprehensive and overarching reforms to the digital regulatory landscape. Reset Australia strongly believes that this comprehensive approach — involving consumer protection and competition law, privacy laws and online safety regulations — is key to creating a digital world that enhances Australian democracy and improves lives.

Reset Australia has previously outlined five directions of for future policy to ensure Australia arrives at an effective, coherent tech regulation framework:

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 narrow set 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 sector-by-sector 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 regulation for the sector.

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.

We warmly welcome the establishment of a digital regulators forum, and believe that further connections across the ACCC, OIAC, ACMA and eSafety Commission are needed to fill the regulatory gaps. Either the ACCC's scope could broaden to address the gaps, or potentially some sort of multi-governance arrangement with the OAIC (and potentially eSafety Commissioner) be developed. From a consumer facing side, a single Digital ombudsman as a digital clearing house for complaints and issues, could greatly streamline the situation for digital users.

Against this broader vision for a future regulatory framework for Australia, we welcome the ACCC's ongoing work around ensuring that Consumer and Competition laws play their part.

3. Response to the ACCC's specific questions

Question 1: What competition and consumer harms, as well as key benefits, arise from digital platforms and services in Australia?

- The experience of Australian consumers in the digital world must reflect the full set of rights that they are entitled to, beyond safety and protection to include privacy and freedom from commercial exploitation. Harms happen in the digital world where people's rights are actively thwarted or fail to be advanced. The description of potential harms to consumers described in the working paper is welcome. The ACCC has embraced a broader view of potential harms that extends beyond content harms, noting multiple other potential risks to Australians in the digital environment. We hope this broader view is also adopted by policy makers and other digital regulators.

- While the description in the working paper is thorough and comprehensive, one potential aspect not discussed was the ways that reduced consumer choice can reinforce risks by normalising bad practice. When Reset Australia has spoken to families, parents and to teengers we are often told that risky digital platforms are the 'natural order', and that no other options are possible. It appears that the ability of digital platforms to leverage their market dominance not only stifles innovation, but also the public's belief that a better digital world is possible. Better, more rights respecting digital platforms are possible, and an increase in consumer choice may help catalyse demand.

- Lastly, it is worth noting that for young users, dark patterns can generate very distinctive harms. As the working paper notes, dark patterns or choice architecture involves designing 'user interfaces that take advantage of certain psychological or behavioural biases'. Children have very particular developmental, psychological and behavioural needs that can create additional vulnerabilities to dark patterns. So much so that for young people, dark patterns are increasingly referred to as 'design abuses'. Design abuses are rife in digital platforms designed and used by children; for example navigational restrictions, perceived time pressures and 'parasocial pressures' are routinely deployed on platforms to encourage children as young as three to make purchases[1]. Multiple countries around the world have or are looking at legislation to protect child consumers from these design abuses, including the UK, Ireland, Sweden, the Netherlands, France, the European Data Protection Board, California and the USA[2].

  We appreciate that the Attorney General is proposing an Online Privacy Code that will ensure data processing is undertaken in ways that are in the best interests of children and young people that may address some aspects that these Codes address. However, what the Online Privacy Code – rooted in Privacy Law – may fail to address is exactly

[1] Jennifer Radeski forthcoming 'Design abuses targeting children'

[2] See for example, the UK's *Age Appropriate Design Code* 2020, Sweden's *Children and Young People's Rights on Digital Platforms* 2021, France's *Eight recommendations to strengthen the protection of minors online* 2021, The Netherland's *Code for Children's Rights* 2021, Ireland's *Fundamentals for a Child Oriented Approach to Data Protection* 2021, California's proposed California Age Appropriate Design Code the Federal US' proposed Kids Online Safety Bill and *PRIVCY Bill*

the impact of these sorts of design abuses and dark patterns on children as consumers. Privacy and data protection will not stretch to ensuring that deliberate choice architecture protects children from commercial exploitation.

Australia urgently needs regulation or regulatory guidance to ensure that children are protected from inappropriate design abuses.

Question 3: Should law reform be staged to address specific harms sequentially as they are identified and addressed, or should a broader framework be adopted to address multiple potential harms across different digital platforms and services?

- Where regulations adopt an issue-by-issue approach, harms will always occur. This sort of piecemeal approach leaves regulators downstream of the harms, having to wait until problems arise and cause harms before they can be addressed. Australian policy makers should not be playing 'harms-whack-a-mole'.

- Reset strongly believes that a pro-active, upstream approach is required. Placing broad, open-ended obligations on digital platforms – such as a duty of care, or obligations to reduce risks in the systems and processes – must be a necessary part of the regulatory mix. This approach has two distinct advantages:
    - They can hold platforms accountable for harms they should have reasonably foreseen and mitigated.
    - They can somewhat 'future proof' regulations. Regulations that take an issue-by-issue approach, or sector-by-sector approach, can struggle to keep up with the pace of development for new technologies and new risks. For example, existing regulations (including forthcoming regulations like the Enhancing Online Privacy Bill) will not address the Metaverse, potentially the single most transformative digital experience for Australians over the coming few years. However, duties of care can.

  Broader frameworks, with clear guidance and strong enforcement can help to reduce harms.

- We also note that this aligns with emerging international regulator consensus, including the EU and UK. Introducing similar, comparable requirements into Australian regulations could harmonise regulations and reduce friction for Australian companies looking to offer global

Question 4: What are the benefits, risks, costs and other considerations relevant to the application of each of the following regulator tools to competition and consumer harms from digital platform services in Australia:

a) prohibitions and obligations contained in legislation
b) the development of code(s) of practice
c) the conferral of rule-making powers on a regulatory authority

d) the introduction of pro-competition or pro-consumer measures following a finding of a competitive or consumer harm
e) the introduction of a third-party access regime, and
f) any other approaches not mentioned in chapter 7.

- When it comes to the methods of regulation, a move towards regulating digital platforms with 'black letter law', or primary and secondary legislation, is long overdue in Australia. Big tech poses big risks and necessitates a robust regulatory response however because we have – to date – largely engaged self- and co-regulatory models, regulation has failed to adequately reduce risks.

- A decade ago, the Australian Government outlined three considerations necessary to determine the nature of the regulatory response an issue warranted[3]. These were:

    1. *The level of risks posed by digital platforms*: Platforms create significant risks, including major public health risks. Taking Facebook and the pandemic as an example, Australia witnessed the enabling and promotion of harmful content and discussions. Both membership numbers and engagement among groups peddling 'anti-vaxx' and vaccine hesitant content grew across the pandemic in Australia[4], with deadly consequences.

    2. *Community interests and expectations of legal sanctions:* There are now legitimate community expectations of explicit regulation of Big Tech in Australia. 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[5], and a poll by the Australian Financial Review in late 2020 found that 77% of Australians felt that BigTech should face stronger Government regulations[6]. The scale and depth of the public's concerns warrants the strongest possible regulatory response.

    3. *The ability of 'the market' to address the issue:* While many sectors have worked hard to deserve the benefit of 'light touch' regulations, digital platforms have demonstrably not.

        Large digital platforms have been found to breached existing privacy and safety regulations repeatedly. YouTube settled a case for $170m USD with the FTC in 2019 for using children's data without necessary parental consent[7]; Google was fined €500m fine for acting in bad faith around EU copyright directives[8], and €220m for anti competitive practices in their advertising

[3] Australian Government 2010 *Best Practice Regulation Handbook* Canberra
[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] Lowry Institute 2021 *Lowry Institute Poll* https://poll.lowyinstitute.org/charts/threats-australias-vital-interests/
[6] Paul Smith 2020 'Big Tech on the Nose' *Australian Financial Review* www.afr.com/technology/big-tech-on-the-nose-as-aussies-demand-accountability-and-tougher-laws-20201030-p56a93
[7] FTC 2019 'Google and YouTube will Pay Record $170m for Alleged Violations of Children's Privacy Law' www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations
[8] Ian Carlos Campbell 2021 'Google fined €500 million in France over bad faith negotiations with news outlets' *The Verge* www.theverge.com/2021/7/13/22575647/google-fine-500-million-french-authorities-news-showcase

systems in France[9]; Facebook settled a complaint with the FTC for a $5b USD for breaching consumer privacy regulations[10] and a $5m USD to settle civil rights lawsuits claiming the company's advertising system was discriminatory[11]; TikTok settling a case for $5.7 m USD with the FTC in 2019 for using children's data without the necessary parental consent[12], and are currently facing a £1b plus lawsuit led by the UK's former Children's Commissioner for excessive data collection practices[13].

Beyond compliance with existing regulations, at times the sector appears to actively resist 'doing the right thing'. For example, back in 2016, the Wall Street Journal found an internal Facebook presentation documenting that they know their platform was hosting a large number of extremist groups and promoting them to its users: "64% of all extremist group joins are due to our recommendation tools," the presentation said[14]. It was only in the wake of the insurrection in January 2021 that Mark Zuckerberg announced that the company will no longer recommend civic and political groups to its users.

This does not reflect a series of unrelated incidents. Most of these companies are publicly listed entities obligated to act in shareholder's best interests. Without legal requirements insisting that they prioritise user safety, they are bound to continue to prioritise shareholder profits. The 'market' is structurally unable to fix the issue.

Digital platforms have exceeded any reasonable threshold for lighter touch self-regulatory or co-regulatory Codes on all three considerations, and self and co-regulatory models need to be ruled out as effective options for future digital regulations in Australia.

- Alongside primary or subordinate legislation, empowering regulators with rule making powers would enable the ACCC, OAIC and eSafety Commissioner to shape the regulatory framework in timely and reactive ways. These powers would be helpful in addition to primary legislation that creates overarching duty of care requirements.

[9] Simon Read 2021 'Google Fined €220m in France' *BBC* https://www.bbc.com/news/business-57383867
[10] FTC 2019 *FTC imposes $5 Billion Penalty* www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy
[11] Brakkton Booker 2019 'After Lawsuite, Facebook Announces Changes' *NPR* www.npr.org/2019/03/19/704831866/after-lawsuits-facebook-announces-changes-to-alleged-discriminatory-ad-targeting
[12] FTC 2019 *Video Social Networking App Settles* www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ft
[13] BBC 2021 'TikTok sued for billions over use of children's data' *BBC* www.bbc.co.uk/news/technology-56815480
[14] Jeff Horwitz & Deepa Seetharaman 2020 'Facebook Executives Shut Down Efforts to Make the Site Less Divisive' *Wall Street Journal* www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507

Question 5: To what extent should a new framework in Australia align with those in overseas jurisdictions to promote regulatory alignment for global digital platforms and their users? What are the key elements that should be aligned?

- A streamlined, overarching digital regulation framework in Australia would consist of three key pillars:

    1. An expanded *Online Safety Act,* including:
        - A more systemic focus on duties to reduce risks in systems and processes (right across the service, and including for example algorithms and ad delivery systems);
        - Expanding the definition of risks to include community and societal risks, which necessitates an enhanced focus on mis/disinformation and hate speech
        - Requiring enhanced duties of care for accountability, and including requirements for transparency measures
        - Replacing voluntary and co-regulatory codes with upstream obligations in the Act
        - Ensuring that the broadest range of digital services remains covered, with risk based additional obligations. (The scope of the *Online Safety Act* is already very broad, and this provides a potential model for other regulations)

    2. An expanded *Privacy Act* and Enhancing Online Privacy Act including:
        - A broader definition of personal data to cover metadata and other new forms of data fuelling the new digital world
        - Adopt a systemic focus on reducing the risks created through the processing of data
        - Apply to the broadest range of digital service providers with risk based additional obligations
        - Replace voluntary and co-regulatory codes with upstream obligations in the Act

    3. Updated CCA & ACL Act, as discussed in this working paper

- Adopting this approach would create a more streamlined approach to regulation, replacing multiple disjointed obligations with more aligned upstream duties and reducing the regulatory burden on Australia's successful tech industry.

- It would also be interoperable with emerging international requirements in the UK & EU, ensuring Australian industry could expand into international markets with minimal regulatory friction. Aligning around duties of care and obligations to protect users fundamental rights would both comprehensively protect Australian consumers and ensure that Australian regulations are broadly interoperable for digital platforms.

Questions 8, 9 & 10: Data access measures and data limitation measures

- Responding to these three questions adequately requires re-thinking digital platform's fiduciary duties to consumers and their data. Consumer's personal data is *owned* by consumers. This places a duty of care on platforms – as data processors – to users as data owners. This duty of care requires digital platforms to process data in consumer's best interests. Personal data is not the property of the digital platforms that collect it, nor can they use it to benefit commercial interests where these interests conflict with user's interests.

- Remedying competition concerns by increasing access to data will harm consumers further *where that data has been collected, processed or shared in ways that do not fundamentally respect consumer's privacy*. The massive competitive advantage that many digital platforms hold has come at the expense of user's privacy and this needs to be addressed. Plainly put, if the way a platform has become too competitive is by breaching user's privacy, the solution is to prevent platform's breaching privacy in the first instance, not to decrease barriers to further data access.

- Revising competition law on the assumption that privacy is perfectly upheld for Australian users will create problems. The reality is that the *Privacy Act* is outdated and subject to an ongoing review, and the OAIC is under-resourced.

- Privacy is a fundamental consumer right, and needs to be protected in the definition of unfair practices in consumer and competition laws.

Question 11: What additional measures are necessary or desirable to adequately protect consumers against:

a) the use of dark patterns
b) scams, harmful content, or malicious and exploitative apps?

- As noted above, children and young people are uniquely vulnerable to design abuses, dark patterns, scams and commercially exploitative digital products. While there is a significant power imbalance between a digital platform and individual users, this disparity is amplified in the case of those under 18.

- Young people are protected by an imperfect mosaic of regulations;
    - from abusive and bullying content by the *Online Safety Act*
    - soon to be protected from pornographic material under the Restricted Access Services regime, and
    - potentially from some of the most egregious uses of their data under the Online Privacy Code

  But they still face significant risks in the digital world. For example, risks of being recommended eating disorder content, of gambling like features in loot boxes, of being recommended 'adult strangers' to befriend and follow, and of being fed extremist materials by social media algorithms remain unaddressed. These risks

emerge from the systems and processes of digital platforms, and are particularly troubling given the rise in mental health issues among the young and the falling age at which people are finding themselves on ASIO's watchlist.

- Exploring what a systemic, risk-based approach looks like for children and young people highlights the range of contextual risks that are inadequately addressed within existing frameworks. The child online safety sector has a commonly used typology that characterises the range of online harms children face; the 4Cs[15]. Figure one contrasts the 4Cs with our regulatory framework.

- As discussed in our response to question 1 multiple countries around the world have or are looking at legislation to protect children comprehensively. The Online Privacy Code and *Online Safety Act* combined will only get us part of the way. Australia urgently needs regulation or regulatory guidance to ensure that children are protected from inappropriate design abuses. We need either a parallel mechanism alongside the Online Privacy Code if it is introduced, or a stand alone Children's Code if it is not.

[15] Sonia Livingstone & Mariya Stoilova 2021 *The 4Cs: Classifying Online Risk to Children, CO:RE Short Report Series on Key Topics* doi.org/10.21241/ssoar.71817

The 4Cs of risk for children and young people against Australia's current regulatory framework

Risk	Some of the current regulatory framework	Gaps in framework
Content — risk of exposure to inappropriate content. For example, risks of exposure to violent content, racist content, pornography, sexualised imagery and mis & disinformation	The *Online Safety Act 2021* is establishing frameworks and Codes around class 1 and 2 materials, as well as developing a Restrictive Access System to limit access to age inappropriate materials like pornography. Violent online material may be addressed by the *Sharing Abhorrent Violent Material Act* 2019	Regulation focuses on individual pieces of content, and overlooks the role of platforms in promoting harmful content to children (via algorithms, for example. Hate speech, mis & disinformation are not adequately addressed in the current framework, but can be harmful
Contact — risks of making inappropriate contact with others. E.g. Risks of exposure to online grooming, stalking & extremist recruitment	A number of online laws exist that address contact risks, from the *Criminal Code Amendment (Protecting Minors Online) Act* 2017 to laws around terrorist recruitment. Some of the *Online Safety Act's* co-regulatory codes around ensuring user safety may address ways platforms can reduce contact risks. These are as yet unpublished and will be authored by industry	Existing legislation remedies some harms but does not mitigate risks. While they may criminalise individuals who make inappropriate contact, they do not require platforms to stop recommending adult strangers as 'friends' or 'followers' or prevent platforms enabling adult accounts to message children's accounts for example
Contract / Commercial — risks arising from inappropriate commercial activities and contract exploitation. E.g. risks of identity theft, gambling, profiling bias, surveillance advertising, persuasive design	Children's data is protected as adult's data under the *Privacy Act 1988*, which may reduce the risk of identity fraud. The Online Privacy Code may reduce commercial risks to children's data, but it is yet to be published and will most likely be authored by industry. The Restrictive Access System may restrict gambling (but may miss loot boxes in games).	The use of children's data poses significant risks, and it is unlikely that an industry drafted code — penned by a sector that funds itself through the commercial exploitation of data — will draft a code that puts children's best interests first. There is no regulation in Australia that addresses dark patterns or persuasive design
Conduct — risks associated with inappropriate behaviour. E.g. bullying, trolling, joining harmful groups (e.g anti-vax)	The *Online Safety Act* includes specific provisions around cyber-bullying for children under 18. This includes taking down content that is deemed cyber bullying, and where the perpetrator is a child, the regulator is able to require apologies	Engagement with harmful communities falls outside the scope of current regulatory frameworks

Question 12: Which digital platforms should any new consumer protection measures apply to?

- Regulations that cover all digital platforms create fewer spaces for gaps and inconsistencies, but larger online platforms must carry additional responsibilities proportionate to the additional risks they pose. In reality, this means we would like to see broad regulation requiring all digital services to address risks in their systems and process, but placing extra obligations to identify and mitigate risks for platforms with more than 2.5m Australian users

Question 16: In what circumstances, and for which digital platform services or businesses, is there a case for increased transparency including in respect of price, the operation of key algorithms or policies, and key terms of service?

a) What additional information do consumers need?
b) What additional information do business users need?
c) What information might be required to monitor and enforce compliance with any new regulatory framework?

- While additional information for consumers and business is always welcome, transparency without choice will lead to few meaningful changes. The efficacy of this approach may be even further hampered by choice fatigue among consumers.

- Placing legislative requirements on digital platforms to proactively disclose risks in systems and processes, including algorithms and complaint mechanisms for example, could produce meaningful changes. Where digital platforms are not transparent about the risks and harms of their businesses, it becomes difficult for regulators to effectively hold them to account.

- Legislative requirements could also create duties for create and public release:
    - Data impact assessments
    - Online safety risk assessments
    - Algorithmic audits and assessment
    - Automated decision making risk assessments
    - Broader AI impact assessments

  These assessments need to consider the unique risks posed to vulnerable users (especially children and young people, different genders, different ethnicities, and the LGBTIQ+ community) and their impact on user's human rights. While these may be of interest to individual consumers and businesses, they would potentially be a more powerful tool to enable regulators (and civil society) to better understand the nature of the risks digital platforms are creating.