Reset.
AUSTRALIA

Submission to the Joint Select Committee on Social Media and Australian Society

Reset.Tech Australia
June 2024

Contents

Committee Secretary
Joint Select Committee on Social Media and Australian Society

Via Email: socialmedia.joint@aph.gov.au

27th June 2024

Reset.Tech Australia thanks the Committee for the opportunity to lodge a submission on the vital issue of social media and society. Meaningful and comprehensive reform of digital platforms has become urgent. We specialise in independent and original research into the social impacts of technology and regulatory models that anchor the public interest as a primary consideration. We are the Australian affiliate of Reset.Tech, a global initiative working to counter digital harms and threats. Our networked structure opens up strong comparative possibilities with other jurisdictions, such as the EU, where the *Digital Services Act* (DSA) and *Digital Markets Act* are in operation, the UK, which has just passed an *Online Safety Act* and a *Digital Markets, Competition and Consumers Act,* and Canada, where an Online Harms Bill has been introduced to Parliament.

Australia has a proud history as a 'first-mover' and innovator in digital platform regulation. Australia was the first country to legislate for online safety and introduce an online safety commissioner,[i] as well as the first to legislate for negotiations between digital platforms and news providers.[ii] Analysis from the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry Final Report*[iii] continues to influence cutting-edge policy thinking locally and internationally.[iv]

In the intervening years, however, **Australia has slipped behind on digital regulation, with digital threats evolving and scaling up in ways that seemed almost unimaginable only a few years ago.** New risks, driven by increasingly powerful algorithms and an explosion of data harvesting, have now surpassed the ability of existing digital regulatory frameworks to effectively manage them. Australia is not alone in facing these risks, but other countries are now making substantial progress, in particular the UK[v] and the EU,[vi] with emerging progress in Canada.[vii] These jurisdictions have drawn upon the innovations and exemplars of Australian policy but introduced more comprehensive, preventative and muscular regulatory models. These models encourage platform conduct that ensures user safety and is more commensurate with public expectations for digital regulation more broadly. By contrast, **Australia is still largely reliant on a hopeful but outdated desire for industry-led and largely self-regulated processes.**

Harm happens as governments wait for self-regulation and co-regulation to fail. Nine years on from the first online safety legislation and five years on from the 2019 ACCC Inquiry, Australia has a new government and faces new digital challenges. A non-exhaustive list includes:

- Personalised and persistent scam calls, texts and advertisements linked to digital advertising business models, causing significant economic harm to Australians;[viii]
- Ongoing risks of online harms for children,[ix] including online exploitation;[x]
- Increasing cyber abuse directed at adults, especially women,[xi] and hate speech directed at minorities;[xii]
- Vast and invasive data breaches, exacerbated by Australia's weak privacy and data protection laws, widening existing holes in national and personal security;[xiii]

- Implementation challenges over the *News Media Bargaining Code*, with Meta's exit from the deals threatening a loss of over $100m to the Australian news market;[xiv]
- A deteriorating information environment, with upticks in 'fringe' and palpably false content, including a rise in AI-generated content with unclear provenance;[xv]
- Governance challenges to DIGI's *Australian Code of Practice on Misinformation and Disinformation*, with X (formerly known as Twitter) exiting the Code after routine failures to respond to independent reports of serious breaches;[xvi] and
- Deepening national security threats of ideologically motivated extremism,[xvii] with intensifying links to content recommender systems (or algorithms).[xviii]

Over the last decade, governments at home and around the world have also learned that:

- Voluntary or, at best, co-regulatory schemes do not produce high-quality protections for Australians[xix] and can simply be ignored by platforms. The 'reputational risk' approach, once held as sufficient incentive for voluntary public interest safeguards, is simply not enough;[xx] and,
- Even legislation and fine regimes are vulnerable to dismissal by very large platforms if they are not considered significant.[xxi]

Summary of Recommendations

Australia urgently needs a comprehensive regulatory model that addresses the underlying *systems* of digital platforms, rather than continuing to rely on content-based regulatory responses. This regulatory model should include *all five building blocks*, namely:

1. An overarching duty of care owed by digital platforms to Australian users;
2. Requirements for platforms to assess all their systems and elements for a defined set of risks;
3. Requirements for platforms to implement reasonable steps to mitigate each risk;
4. Five sources of transparency, including annual risk assessments, prescriptive public transparency reports, independent audits of risk assessments and transparency reports, data portals for ad repositories and content moderation decisions, and researcher access to public interest data; and
5. Enforceable regulations and empowered regulators to compel behavioural change.

These need to be implemented alongside a reformed and updated *Privacy Act* that protects Australians from predatory digital business practices. The proposals put forward in the *Privacy Act Review Report*[xxii] are strong and move in the right direction. These are needed to mitigate the personal and national security risks that social media platforms and other digital platforms routinely generate.

Thank you for considering our submission. We would be delighted to engage further if of use to the Committee.

Yours faithfully

Alice Dawkins
Executive Director

Dr Rys Farthing
Director, Policy & Research

Contact: hello@au.reset.tech

Responses to Terms of Reference

(a) the use of age verification to protect Australian children from social media

Age verification is a necessary ingredient for an online safety framework, but age assurance does not make platforms safe. We note how age verification is typically and routinely invoked by industry as a 'wedge issue' that has the effect of splintering the digital rights and digital accountability of communities, introducing politicised tensions and pulling focus from issues of serious corporate responsibility to 'complexity traps' of technical implementation.

Age verification is a contentious and technically complex issue, but even if these issues are resolved, age verification leaves most digital risks unaffected. Age verification does not make digital platforms safer. It helps address two important issues: keeping users under the minimum age of a social media platform from 'sneaking in', and preventing users under 18 years from accessing pornography on social media platforms. However, it is not a comprehensive approach, as most risks remain unaffected even if age verification is implemented.

Comprehensive frameworks centred on defined systemic risks and prescribed corporate accountabilities are the only way to effectively handle safety concerns. These frameworks require five 'building blocks' (see **Recommendations**). A practical consequence of a comprehensive, risk-based framework is evident in the recent enforcement action opened against Meta in Europe regarding harms to minors.[xxiii] The five building blocks of transparency, accountability, risk assessment, risk mitigation and enforcement put digital platforms on notice to manage defined risks to children and young people on their services and face serious consequences for failure. Platforms are under no defined obligations with regard to their systems and processes for Australian users.

(b) the decision of Meta to abandon deals under the News Media Bargaining Code

The *News Media Bargaining Code* was drafted in a difficult context and, we believe, affected by bad faith negotiation tactics from both Meta and Google. The political context was fraught: Google published and promoted an open letter to all its Australian users that was described as misleading,[xxiv] while Facebook responded by 'turning off the news' in the broadest way possible, allegedly to deliberately cause havoc.[xxv] We have documented this timeline of underhand tactics with the public drafts of the Code, which suggests a correlation between the deployment of underhand tactics from platforms and concessions in the emerging Code.[xxvi]

The resulting instrument relied heavily on corporate goodwill rather than meaningful enforcement. The unceremonious nature of Meta's exit from the Code and the Government's tentativeness to press the 'kill switch' of designation (the as-yet unused enforcement mechanism of the Code) gives a 'voluntary' flavour to the instrument. Regulations or codes targeting large digital platforms need enforceability as a central tenet rather than an afterthought with layered-upon conditions.

This example should not be seen as an isolated incident. When regulation relies on voluntary and 'co-regulatory' mechanisms that allow industry – saddled with significant conflicts of interest – to decide, users' best interests fail to be prioritised (see Figure 1).

- Voluntary requirements have been ignored. For example, despite being a signatory to the voluntary *Australian Code of Practice on Disinformation and Misinformation*, which places clear obligations on platforms to enable end-users to report misinformation,[xxvii] X turned off the ability for Australians to report misinformation two weeks ahead of the Voice referendum.[xxviii]
- Co-regulatory processes see requirements watered down. For example, the Basic Online Safety Expectations (BOSE) in the online safety framework clearly state that default privacy and safety settings for children must be robust and set to the most restrictive level,[xxix] defining a child as

someone under 18 years of age.[xxx] However, because the BOSE are not enforceable and 'come to life' via industry-drafted code-making processes, the actual safety standard in Australia sets default privacy settings and safety standards to the most robust and restrictive only for those under the age of 16 years on social media platforms. This was a deliberate choice by the code drafters, leaving 16- and 17-year-old Australians unprotected.[xxxi]

Figure 1: Examples of failings of voluntary and co-regulatory mechanisms outside of the News Media Bargaining Code

(c) the important role of Australian journalism, news and public interest media in countering misinformation and disinformation on digital platforms

The underlying systems of digital platforms presently receive very little scrutiny in Australia, despite giving rise to a range of risks, including but not limited to mental health impacts. Technologies and content trends change, but the risks caused by platform systems remain relatively constant. For this reason, Australia would be well-placed to follow international best practice by adopting a systemic regulatory model that places positive obligations on digital platforms to mitigate risks across their products and services and be accountable for both the design of systems and elements *and* the impact on the public.

Fact-checkers play a crucial role in securing Australia's information architecture, but Australia's fact-checking ecosystem, largely run by news outlets and academia, is uniquely small and brittle.[xxxii] They face a number of challenges:

- **Size**: We have a modest pool of Australian fact-checking organisations, although international fact-checking organisations may cover some relevant issues.
- **Trust**: A lack of trust and perceptions of bias[xxxiii] pose a risk to this ecosystem.
- **Worsening situation**: The rise of generative AI poses a risk to their functionality. Detecting deepfakes and other misinformation generated by AI is a labour-intensive task. There are no sufficiently accurate automated tools to do this independently of human analysis, and each piece of content flagged for fact-checking requires human and technical analysis to assess credibility. Australia's pool of fact-checkers have their work cut out, as bad actors turn to readily available off-the-shelf generative tools to create political deepfakes.

We have also seen a disturbing new trend where bad actors have been explicitly attempting to 'overload' Australian fact-checkers by flooding them with requests to fact-check the same (or similar) pro-Kremlin fake videos.[xxxiv] In effect, this is a new variant of a Distributed Denial of Service attack, except instead of disrupting the flow of traffic by overloading a server with requests, it attempts to overwhelm fact-checkers with a flood of requests that require excessive time to address. This trend has taken a new twist, with these overload requests now being sent via scannable QR codes containing potentially malicious code.[xxxv] The brittleness of Australia's fact-checking industry renders it vulnerable to AI-supercharged bad-faith attacks and security risks designed to disrupt and undermine trust in institutions.

Beyond the difficulties and limitations of the fact-checking landscape, it remains unclear how effective digital platforms' responses to third-party fact-checking really are. In response to a complaint about inconsistencies in their annual transparency report under the *Australian Code of Practice on Misinformation and Disinformation,* Meta clarified how narrow and limited their response to a third-party fact-check is in practice. Like other platforms, Meta only label or remove the exact post that fact-checkers address and near-identical copies. Posts that repeat the same falsehoods, attach images or swap the order of words remain unaffected even when reported (see Figure 2). To provide an indication of the limitations of this approach, the three Australian-focused third-party fact-checkers that Meta works with – the AFP, AAP and RMIT FactLab[xxxvi] – fact-checked a total of 37 'original posts' in May 2024.[xxxvii] These ranged from a claim that France had imposed martial law on New Caledonia[xxxviii] to a claim that Greta Thunberg is a Rothschild.[xxxix] Save for the existence of non-publicly listed fact-checks, this means that in May 2024, only 37 original posts and copies and near-identical copies of these posts would have been removed from 'Australian-specific' Facebook. While Meta's responses to international fact-checking also affect what Australians see and consume, this leaves us reliant on an international

fact-checking community that, by definition, lacks domestic nuance and raises issues of sovereignty. Clearly, this approach is not desirable and will struggle to meet the scale of the accelerating risks.

This is a fact-checker's finding

This content is not labelled despite containing fact-checked misinformation because it was not the exact post the fact-checker reviewed[xl]

Figure 2: An example of content that will not be labelled despite a fact-checker's finding

Furthermore, the response to the complaint from the Code's sub-committee under their complaints procedure worryingly suggests that digital platforms are, de facto, permitted by the process to mislead the public in their annual reports on misinformation and disinformation mitigation measures.[xli]

(d) the algorithms, recommender systems and corporate decision-making of digital platforms in influencing what Australians see, and the impacts of this on mental health

The underlying systems of digital platforms presently receive very little scrutiny in Australia, despite being the most significant factor in generating or mitigating risks within the digital ecosystem for Australians. Risks arise from a range of platform systems, including algorithms and recommender systems. However, these risks are not limited to these elements. For example, previous research has shown how recommender systems, content moderation systems, advertising approval systems and targeted advertising systems[xlii] can exacerbate risks such as eating disorders and contribute to negative mental health impacts. Additionally, these systems can lead to other harms, including intra-family conflict, financial losses from scams and the polarisation of political discourse through rabbit-hole effects. For these reasons, Australia would be well-placed to follow international best practices by adopting a systemic regulatory model that is comprehensive and places positive obligations on digital platforms to mitigate risks across their products and services. Such a model should hold platforms accountable for both the design of systems and their impact on the public. We outline this model and its 'five building blocks' of duty of care, risk assessment, risk mitigation, transparency and enforceability below.

Building Block 1: A Duty of Care

Ensuring that digital platforms play their part in reducing the risk architecture requires 'flipping the table' from older models of regulation, where end-users shoulder the bulk of the risk, and instead placing responsibilities onto digital platforms to keep end-users safe. Learning from international models, placing a duty of care on digital platforms could help drive the systemic and preventative focus that is urgently needed in Australia.

A duty of care approach is a way to implement systemic regulation that moves the focus beyond the content layer of the digital world to the underlying systems: the environment where content is created, shared and promoted. The design of these underlying systems is entirely within a platform's control (to a lesser extent where content is generated by users). Focusing regulation on systems and processes requires platforms to assess whether there is a risk of harm to users arising from their technical systems, design and business models, while still encouraging user expression.

Focusing on design and operation is important because despite their name, 'platforms' are not entirely neutral, passive transmitters when it comes to content. Intentionally or not, their choice architecture impacts content. This includes the role of recommender and content moderation systems, for example, and how engagement features are designed to create social pressures or allow for anonymous accounts. Duty of care is a way to implement systemic regulation that can address these types of risks.

Duty of care is a familiar model for risk management in Australia, with established frameworks in workplace health and safety. An online statutory duty of care exists in the UK's *Online Safety Act* (OSA)[xliii] and is contemplated in draft Canadian legislation, the Online Harms Bill.[xliv] We note that proposals for a duty of care in Australia should be mindful of the British experience and avoid being 'watered down' into pluralised duties of care. Introducing duties of care rather than a singular duty of care reduces the systemic focus and introduces content-focused confusions and limitations into regulation.[xlv]

Building Block 2: Risk Assessment

Once responsibility has been placed onto digital platforms to safeguard end-users, requirements to produce risk assessments could introduce a comprehensive focus into the regulatory framework. This approach has strong international precedent; requirements to produce risk assessments for systemic risks on digital platforms exist in both the EU's DSA[xlvi] and the UK's OSA.

Currently, risk assessments are part of the Australian BOSE, although they are suggested as an example of a reasonable step to address specific risks covered by the BOSE; they are neither mandatory nor comprehensive. In addition, the Office of the eSafety Commissioner has created a world-leading Safety by Design assessment tool, which serves as guidance and advice for digital product developers.[xlvii] While this tool has significant strengths, it is a self-assessment tool linked to a set of safety risks and was not designed to support regulatory enforcement.

Requirements to produce risk assessments could ensure that platforms adequately review and identify the risks that their systems and processes create. As the Centre on Regulation in Europe describes, risk assessment activities begin with a comprehensive mapping activity that identifies the ecosystem in which platforms operate, the roles and behaviours of users, business decisions made by platforms and how these interactions produce risks.[xlviii] In other words, risk assessments have the capacity to encourage digital platforms to think comprehensively about how their platforms can create or amplify risks.

Building Block 3: Risk Mitigation

The responsibility to identify a comprehensive, systemic set of risks can be preventative when digital platforms are required to actively mitigate and minimise the likelihood and severity of these risks. This way, platforms can be incentivised to implement changes that prevent harms from occurring in the first instance. In this sense, as the idiom goes, risk mitigation measures are the equivalent of 'placing a fence at the top of a cliff rather than ambulances at the bottom'.

Again, a strong international precedent exists for risk mitigation requirements. The EU's DSA[xlix] and the UK's OSA place obligations on platforms to mitigate identified risks, and Canada's Online Harms Bill also imposes obligations on platforms to mitigate risks aligned with their duties. Currently, risk assessments that include risk mitigation measures are part of the Australian BOSE, although they are suggested as an example of a reasonable step in response to a range of risks covered by the BOSE and are not mandatory.

We have seen requirements for risk mitigation measures begin to bring about positive changes overseas. For example, the European Commission has opened formal proceedings against Meta for failing to adequately identify risk mitigation measures to curb harm to minors, and for failing to adequately adopt mitigation measures regarding visibility around political content and flagging illegal content, among others.[l]

The DSA specifically outlines a set of 'mitigation measures' that could be expected from digital platforms, such as:

- Changing the design, features or functioning of their services, including their online interfaces;
- Changing terms and conditions and their enforcement;
- Changing content moderation processes;
- Testing and changing algorithmic systems, including recommender systems;
- Changing advertising systems, including the way ads are targeted at or presented to people;
- Improving internal business processes to maximise safety;
- Collaborating with other digital services;
- Taking targeted measures to improve child safety, such as age assurance or parental control tools; and
- Ensuring evidence about potential illegal activities is stored and reported in helpful ways to law enforcement.[li]

Australian expectations could harmonise with EU requirements to reduce the compliance burden on platforms. This would introduce a robust mechanism that encourages platforms to implement preventative measures and allows regulators to meaningfully interrogate proposed measures while they are still risks rather than actualised harms.

Building Block 4: Transparency

Regulating for transparency helps address the power asymmetry of large digital platforms by making some of the information necessary for understanding online risks visible to the public and regulators. This enables individuals to make informed choices about platform use and allows regulators to take action. Current Australian measures for transparency in the online safety framework stem from requirements in the BOSE. Under the BOSE, the Office of the eSafety Commissioner has the power to request a range of information from platforms through periodic and non-periodic 'transparency notices'.[lii] While responses to these notices are sent directly to the Office of the eSafety Commissioner, the Commissioner is empowered to publish a statement regarding reports on their website, which serves a subsequent public transparency function.[liii] Platforms have not always adequately responded to these requests,[liv] and these requirements for transparency are modest compared to overseas regulatory benchmarks.

Internationally, transparency requirements are stronger in other markets with regulation. For example, the DSA introduces five key types of public transparency measures: annual risk assessments released in summary form to the public after a period of time, highly prescriptive annual transparency reports sharing detailed data about platform functioning, annual independent audits, data portals including ad repositories and content moderation data and researcher access to public interest data.[lv] Similarly, the UK OSA introduces two key public transparency measures: annual risk assessments and annual transparency reports.[lvi]

Learning from this, Australia could adopt a model of transparency that includes requirements for summaries of risk assessments to be published, annual prescriptive transparency reports, annual independent audits, data portals and researcher access (see Figure 3).

Building on the model under the DSA,[lvii] Australian researchers could have mandated access to platform data. In Australia, requirements for an Australian vetted researcher could include:

- Affiliation with a research organisation, including academic and third-sector research organisations;
- Researchers, or at least the lead researcher, should be an Australian resident or citizen; and
- Non-commercial purpose limitations.

Suitable research projects should be provided with data. A suitable project proposal would include information demonstrating that:

- The research aligns with the objectives of the relevant legislative instrument (such as the *Online Safety Act*) and is broadly of public benefit. This excludes data concerning trade secrets;
- Funding for the research is fully disclosed;
- Access to the specific data requested, and the indicated timeline, is necessary and proportionate to the research purposes;
- Data security, confidentiality and personal data safety requirements will be met; and
- The research results will be publicly available free of charge within a reasonable period after completion.

The process for requesting data could be managed by the Australian Communications and Media Authority, the Office of the eSafety Commissioner or another appointed independent organisation. In addition, existing data and data tools like APIs should be made available to Australian researchers free of charge.

Figure 3: A potential researcher access scheme for Australia

Building Block 5: Accountability from Enforceability

As seen with the current co-regulatory and voluntary approach, where platforms have an outsized role in setting their own standards, the best interests of end-users are not prioritised. Enforceability is key, yet comparatively weak in Australia. International regulators possess a range of enforcement powers that are not currently available to the Office of the eSafety Commissioner to compel redress. Enforcement powers should include the ability to issue significant fines for failures to meet required improvements. Figure 4 highlights the scale of the fining regime available to comparable regulators. Furthermore, strong last-resort measures are needed to prevent platforms from disregarding regulators' requests. International examples of last-resort measures include:

- Under the DSA, in cases of significant and persistent failures where attempts at engagement have failed, regulators can 'turn off' services. Specifically, the DSA outlines that if an 'infringement has not been remedied or is continuing and is causing serious harm, and that infringement entails a criminal offence involving a threat to the life or safety of persons', regulators can work with domestic courts to order temporary restrictions of access.[lviii]
- Alternatively, under the UK OSA, with the agreement of the courts, Ofcom can require payment providers, advertisers and internet service providers to stop working with a site, preventing it from generating revenue or being accessed from the UK.[lix]
- In extreme cases in the UK, criminal sanctions can be imposed on senior management if transparency measures are not met. The UK OSA requires companies to identify senior managers who are liable for responding to information notices. Failure to comply with an information notice request is a criminal offence.[lx] These measures stand in stark contrast to Australian enforcement powers, where requests for information have been ignored and fines of $610,500 issued.[lxi]

- Under the UK OSA, companies can be fined up to £18 million or 10% of their qualifying worldwide revenue, whichever is greater.
- Under the DSA, companies can be issued penalties of up to 6% of global annual turnover for failure to effectively mitigate risks and up to 1% of global annual turnover for supplying incomplete or misleading information as part of meeting transparency obligations.
- In Australia, regulators in adjacent domains of consumer protection and financial services have comparable fining abilities. For example, the ACCC can fine up to 10% of annual turnover for franchising violations,[lxii] and ASIC can fine up to 10% of annual turnover, capped at $782.5 million, for violations of ASIC-administered legislation.[lxiii]

Figure 4: Fining regimes available to other regulators

(e) other issues in relation to harmful or illegal content disseminated over social media, including scams, age-restricted content, child sexual abuse and violent extremist material

The issues listed here are clear examples of digitally enabled financial security risks, child safety risks and national security risks. These types of risks are often generated and routinely exacerbated by the underlying systems deployed by digital platforms. Refer to our response to (d) for the five building blocks required to regulate digital platforms for safety with a risk-based approach and a systemic focus. It is vital to note that regulating systemically will reduce a range of interconnected risk vectors, but this needs to be augmented and reinforced by strong regulation that also addresses consumer and competition angles and, importantly, privacy concerns. Even the most comprehensive application of online safety regulation will struggle to encompass all aspects of market-driven digital risks. For example, see our response to (f) on how financial security risks, child safety risks and national security risks are dramatically worsened by archaic privacy laws and poorly regulated data markets. Meaningful accountability for social media companies requires the government to take deliberate regulatory actions that cut through the power dynamics of data firms and digital markets,[lxiv] by protecting consumers through reformed consumer protection and privacy laws and setting clear guardrails for corporate conduct.

(f) any related matters

The Integral Role of Privacy

The need for comprehensive privacy reforms for Australians is serious and urgent. Research into the nexus of digital platforms and data brokers highlights the breadth of personal information collected about Australians each day, which is truly breathtaking.[lxv] Much of this data is identifiable but currently sits beyond the scope of the *Privacy Act*, meaning it is unprotected in its collection, use and disclosure.[lxvi] The scale and impact of data breaches highlight the substantial risks posed by unregulated data collection practices. Given the breadth of nefarious actors, from scammers who buy and use personal data to trick victims (see Figure 5) to foreign agents weaponising this data,[lxvii] Australia's outdated privacy laws enable significant and unnecessary personal and national security risks. Social media platforms – and their parent companies – are key drivers of these risky data practices. Indeed, this is their business model. Social media platforms exist, from a business perspective, to facilitate and profit from data-driven ad-tech that parent companies derive their profit from.

These practices pose risks for children and young people. Children's personal data is often collected en masse, creating significant and lifelong risks. For instance, 'safety' apps selling children's live location

data[lxviii] and EdTech apps tracking high school students' digital activities for advertising purposes[lxix] are prevalent examples. Children's data is widely collected and traded in an unregulated fashion, already exploited by advertisers.[lxx] With the rise of Generative AI and its substantial data requirements, the misuse of this data could create lifelong risks for young people.

The risks posed by poorly regulated data practices are widespread and profound. Limited interventions focusing on interpersonal harms, such as efforts to address doxxing, will not adequately tackle the fundamental issues of corporate conduct. The proposals presented in the *Privacy Act Review*[lxxi] in February 2023 are bold and necessary, arising from a series of consultations held from 2020 onward across various governments. An *Issues Paper*, a *Discussion Pape*r and a *Review Report* were all developed and consulted on, with the resulting proposals being evidence-based, well-informed, necessary and supported by the Australian public. Nine months have passed since the Government issued its response to the review, announcing its intention for a broad and comprehensive overhaul. Now is the time to implement these proposals to ensure Australians are safer and more secure in a digital context.

Part of the reason scams have become an increasing issue over the last decade is how deeply deceptive and undetectable they have become. This is particularly true for impersonation scams, such as bank scams, utility provider scams, parcel delivery scams or tollway scams, where scammers contact victims and pretend to be from their bank or another legitimate company. One reason people are vulnerable to these scams is that scammers often possess extensive information about their victims, creating an illusion of legitimacy. For instance, in its consumer guidance on identifying scams, the ACMA advises that it is likely a scam if 'someone you don't know has your personal details. A scammer might have stolen your personal details and use them to convince you they are a trusted business (for example, pretending to be your bank or telco provider)'.[lxxii]

While some scammers may have indeed stolen this data or accessed it through data breaches, this is a comparatively circuitous and inefficient route. Data about people's banking providers and habits are widely and easily for sale without strong vetting procedures. This data can be purchased alongside other information, such as recent online purchases, the type of car they own or the ages of their children. For example, the Xandr file documents how data about customers of NAB, Suncorp, Westpac, AMP Bank, BankWest, CommBank, Macquarie Bank, Adelaide Bank and Allianz could all be legally purchased from Oracle (BlueKai, Datalogix, AddThis). This data can be easily combined with information on household expenditure and geolocation, such as 'recent visits to bank branches' (or even recent trips to Oporto for some chicken and chips), allowing scams to appear very realistic.[lxxiii] It is unclear why scammers would rely on incomplete, harder-to-access stolen data sources to personalise scams, when Australia's data brokering market freely and legally trades this data.

Figure 5: The relationship between the widespread collection of data in the digital realm (including on social media platforms) and advertisers

The Public Supports Brave and Systemic Action

Working with YouGov, in April 2024, we polled 1,514 people to gather their views on digital regulation. We found broad support for systemic and comprehensive action. First, there was strong recognition that the public felt unsafe online. In total, 81% of Australians occasionally, regularly or always feel unsafe online (see Figure 6).

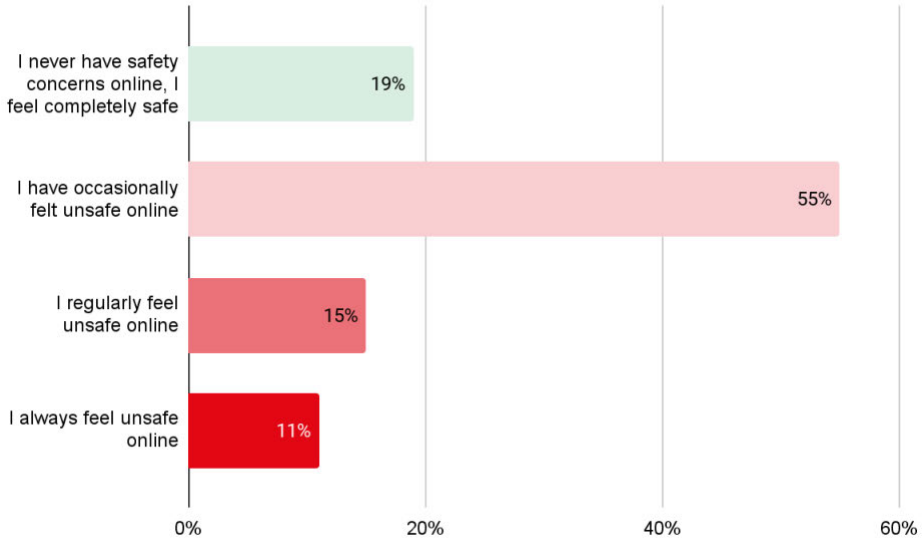

Figure 6: Responses to the question 'Thinking about your experiences using social media platforms, how would you describe your feelings of safety from online risks, such as online scams, deep fakes, data breaches, misinformation and disinformation?' (n=1,514)

When it comes to the type of regulation the public would like to see, there is a strong preference for systemic regulation in conjunction with content-focused regulation (see Figure 7). We asked respondents which 'ways' they would like laws to be drafted and found a preference for systemic and content-focused approaches.

Laws that focus on risky content, leading to its removal once identified	*9%*
Laws that focus on systems, requiring platforms to build better and more effective ways to manage risky content	*20%*
Focus on both risky content and systems	*60%*
Neither of the above options	*3%*

Figure 7: Responses to the question 'There are a number of ways that laws can be made to try to improve online safety. Which of these would you prefer?' (n=1,514) ('Don't know' responses not shown)

We were also interested in understanding if people were concerned about 'over-zealous' content moderation in regulating online content. This did not appear to be the case, with only 5% of respondents expressing concern that platforms were doing too much to address risky content online (see Figure 8). This suggests that concerns about online censorship may not be widely held. Reset.Tech Australia also conducted experimental research during the Voice referendum to detect biased over-moderation of 'Vote Yes' or 'Vote No' aligned fact-checked misinformation. We did not find any bias in moderation but observed a significant tendency towards under-moderation of misinformation on social media platforms.[lxxiv]

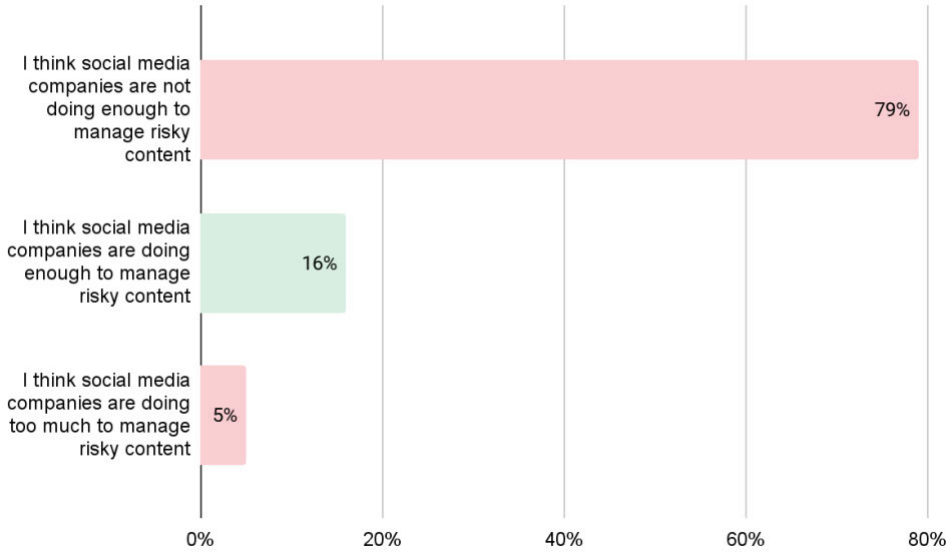

Figure 8: Responses to the question 'Social media companies make lots of decisions about what they do with risky content that breaks their rules. Which of the following best describes how you think social media companies are managing this content?' (n=1,514) ('Don't know' responses not shown)

We asked about our five building blocks approach to digital regulation, beginning with a duty of care. We found strong support for a duty of care, with 93% of respondents agreeing that social media companies should have a duty to take reasonable care of their users (see Figure 9).

Agree	*93%*
Disagree	*5%*

Figure 9: Responses to the statement 'Social media companies should have a duty to take reasonable care of their users' (n=1,514) ('Don't know' responses not shown)

We also asked about measures for risk assessments and risk mitigations, transparency and accountability and found strong support for systemic laws that enhance accountability and transparency (see Figure 10).

Social media companies should have to make thorough risk assessments to identify major risks on their platforms	*59%*
Social media companies should have to take reasonable steps to manage identified major risks on their platforms	*65%*
Social media companies should have to be transparent with the public and regulators about major risks of their platforms	*63%*
Regulators should have the power to compel social media companies to make reasonable changes to their systems to enhance safety	62%

Figure 10: Responses to the question 'It's not always clear if social media companies are responsible for the harms that happen on their platforms. There are some discussions that laws could be passed that make social media companies more responsible. Which, if any, of these responsibility measures would you support in law? (select all you support)' (n=1,514)

We asked for more thoughts about transparency, particularly regarding the ability to 'understand' how platforms' systems and algorithms work. There was support for a range of transparency measures (see Figure 11).

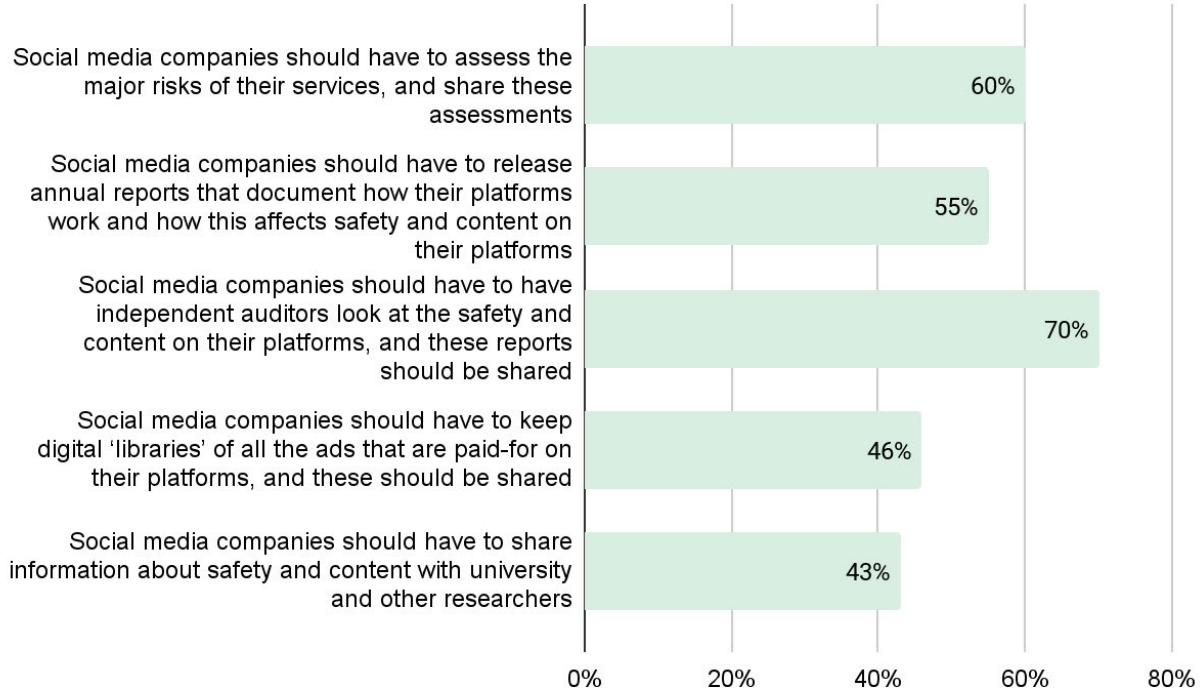

Figure 11: Responses to the question 'It's not always clear how social media companies build their systems and algorithms. There are some discussions that laws could be passed that make social media companies be more transparent about how platforms work and the consequences of this. Which, if any, of these transparency measures would you support in law? (select all you support)' (n=1,514)

Lastly, we also asked about introducing the children's best interests principle into privacy and safety laws and found strong support for its inclusion in both areas. Fifteen percent of respondents thought the children's best interests principle should be in place to protect the use of children's data (privacy), 12% thought it should be in place for online safety rules and 67% thought it should be in place for both (see Figure 12).

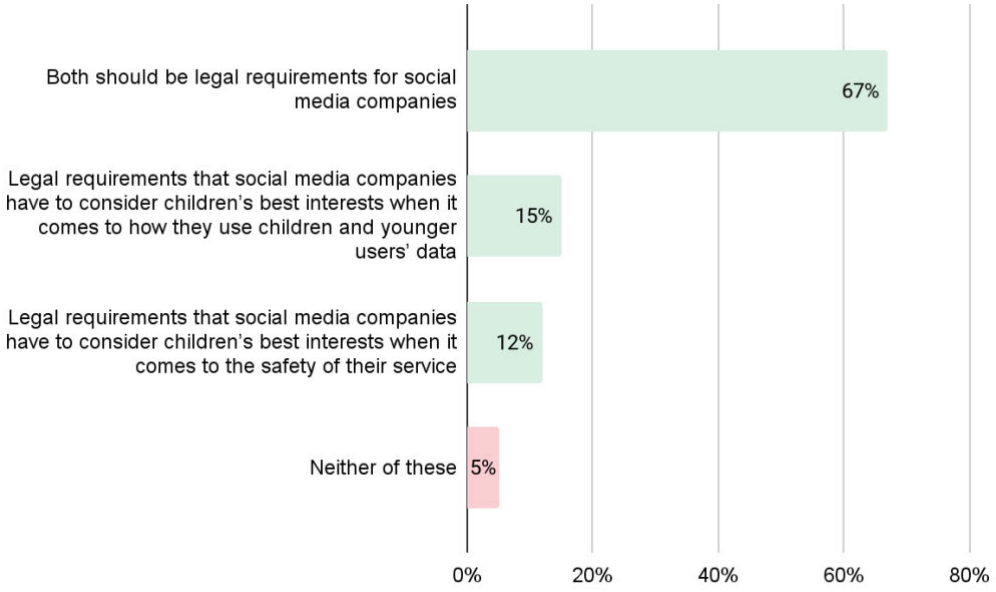

Figure 12: Responses to the question 'It's not always clear if social media companies make their products in ways that are best for children and younger users under 18. There are some discussions that laws could be passed that make social media companies think about children's best interests in the way they work. Which, if any, of these measures would you support in law?' (n=1,514)

Recommendations

Australia urgently needs a comprehensive regulatory model that addresses the underlying systems of digital platforms, rather than continuing to rely on content-based regulatory responses. What is needed is a regulatory model that includes *all five building blocks*, namely:

1. **An overarching duty of care owed by digital platforms to Australian users.** An overarching duty of care would place broad obligations on platforms to ensure user safety in systemic ways. Specific responsibilities could be enumerated by focusing requirements for risk assessments.

2. **Requirements for platforms to assess all their systems and elements for a defined set of risks,** such as risks related to distributing illegal materials, dissemination of scams, electoral processes, civil and political rights, gender-based violence, children's best interests, public health and personal security. These requirements would incentivise systemic change and help platforms realise their duty of care.

3. **Requirements for platforms to mitigate each risk**. As a corollary of risk assessments, platforms must be required to implement reasonable steps to mitigate each identified risk. These measures must be included in the assessments sent to regulators.

4. **Five sources of transparency,** including annual risk assessments, prescriptive public transparency reports, independent audits of risk assessments and transparency reports, data portals for ad repositories and content moderation decisions, and researcher access to public interest data. These need to exist alongside strong investigative powers for regulators.

5. **Enforceable regulations and empowered regulators to compel behavioural change**. This means regulators are empowered and resourced to:
    - Compel redress and changes to platforms' systems and elements rather than just compel transparency or takedown;
    - Issue penalties that match the scale of global profits of digital platforms;
    - Have powers to 'turn off' services where failures are persistent and all other measures have been exhausted;
    - Enhance the public-facing complaints mechanism to include complaints from individuals and consumer groups regarding systemic risks and breaches of duty of care;
    - Have strong investigative and information-gathering powers; and
    - Have effective notice-and-take-down powers.

Additionally, a reformed *Privacy Act* that protects Australians from predatory digital business practices is essential. Reforms must offer meaningful protections for personal data, including metadata, and impose strict requirements regarding fairness and reasonableness to justify data processing by digital platforms and social media. In particular, these requirements should address the market structure and dynamics of harmful digital business models, as highlighted in the recent ACCC report on data firms.[lxxv] The proposals outlined in the *Privacy Act Review Report*[lxxvi] are robust and a step in the right direction. These are crucial to safeguard personal and national security.

[i] Via the *Enhancing Online Safety for Children 2015* Act https://www.legislation.gov.au/C2015A00024/2017-06-23/text

[ii] Via the *News Media and Digital Platforms Mandatory Bargaining Code 2021* https://www.legislation.gov.au/C2021A00021/asmade/text

[iii] Australian Competition and Consumer Commission's *Digital Platforms Inquiry Final Report* 2019 https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report

[iv] For example, see UK Parliament 2024 *Digital Markets, Competition and Consumers Bill* https://bills.parliament.uk/publications/54208/documents/4421 & Government of Canada 2020 *Towards guiding principles — Diversity of content in the digital age https://www.canada.ca/en/canadian-heritage/services/diversity-content-digital-age/towards-guiding-principles.html &* Government of Canada 2021 *News Media Canada* https://ised-isde.canada.ca/site/strategic-policy-sector/en/marketplace-framework-policy/copyright-policy/submissions-consultation-modern-copyright-framework-online-intermediaries/news-media-canada-nmc

[v] UK 2023 *Online Safety Act 2023* https://www.legislation.gov.uk/ukpga/2023/50/enacted

[vi] EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[vii] Canada 2024 *Online Harms Bill 2024* https://www.parl.ca/LegisInfo/en/bill/44-1/c-63

[viii] National Anti-Scam Centre 2023 *National Anti-Scam Centre in Action Quarterly Update* https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update/national-anti-scam-centre-quarterly-update-march-2024 & Consumer Policy Research Centre 2024 *Singled Out* https://cprc.org.au/wp-content/uploads/2024/02/CPRC-Singled-Out-Final-Feb-2024.pdf

[ix] Ranging from Ed Tech apps that breach student's privacy (see Human Rights Watch 2022 *"How Dare They Peep into My Private Life?"* https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments) to algorithms that serve them pro-eating disorder content (Reset.Tech Australia 2024 *Not Just Algorithms: Assuring User Safety Online With Systemic Regulatory Frameworks* https://au.reset.tech/news/report-not-just-algorithms/)

[x] eSafety Commissioner 2022 *World-first report shows leading tech companies are not doing enough to tackle online child abuse* https://www.esafety.gov.au/newsroom/media-releases/world-first-report-shows-leading-tech-companies-are-not-doing-enough-to-tackle-online-child-abuse

[xi] Office of the eSafety Commissioner 2022 *Women In The Spotlight: How online abuse impacts women in their working lives* https://www.esafety.gov.au/research/how-online-abuse-impacts-women-working-lives

[xii] See, for example, the experience of Indigenous Australians during the Voice referendum at Jack Latimore 2023 'Meta rules online racism against Indigenous people meets community standards' *The Sydney Morning Herald* https://www.smh.com.au/national/meta-rules-online-racism-against-indigenous-people-meets-community-standards-20230815-p5dwqt.html

[xiii] Office of the Australian Information Commissioner 2024 *Notifiable data breaches report* http://www.oaic.gov.au/__data/assets/pdf_file/0021/156531/Notifiable-data-breaches-report-July-to-December-2023.pdf & Reset.Tech Australia 2023 *Australians for Sale Targeted Advertising, Data Brokering, and Consumer Manipulation* https://au.reset.tech/news/coming-soon-australians-for-sale-report/

[xiv] The Hon Michelle Rowland MP, Minister for Communications 2024 *Press Conference* https://minister.infrastructure.gov.au/rowland/interview/transcript-press-conference-sydney-0 & Rod Sims 2022 'Australia's News Media Bargaining Code led the world. It's time to finish what we started' *The Conversation* https://theconversation.com/australias-news-media-bargaining-code-led-the-world-its-time-to-finish-what-we-started-188586

[xv] Tom Rogers 2023 'Highest level of mis-and-disinformation we've seen online': AEC' *Australian Broadcasting Corporation* https://www.abc.net.au/listen/programs/radionational-breakfast/aec-on-referendum-education-campaign-and-misinformation-/102758190; Pranshu Verma 2023 'The rise of AI fake news is creating a "misinformation superspreader"' *The Washington Post* https://www.washingtonpost.com/technology/2023/12/17/ai-fake-news-misinformation/

[xvi] DIGI 2023 *Media Statement* https://digi.org.au/category/media-statement/

[xvii] Australian Security Intelligence Organisation 2022 *Director General's Annual Threat Assessment* https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2022 & Australian Security Intelligence Organisation 2023 *Director General's Annual Threat Assessment* https://www.asio.gov.au/director-generals-annual-threat-assessment-2023 & Australian Security Intelligence Organisation 2024 *Director General's Annual Threat Assessment* https://www.oni.gov.au/asio-annual-threat-assessment-2024

[xviii] Reset.Tech Australia 2022 *Algorithms as a weapon against women: How YouTube lures boys and young men into the 'Manosphere'* https://au.reset.tech/news/algorithms-as-a-weapon-against-women-how-youtube-lures-boys-and-young-men-into-the-manosphere/ & Manoel H Ribeiro *et al.* 2019 *Auditing Radicalization Pathways on YouTube* https://www.researchgate.net/publication/335337464_Auditing_Radicalization_Pathways_on_YouTube

[xix] Reset.Tech Australia 2022 *How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot* https://au.reset.tech/uploads/report_-co-regulation-fails-young-people-final-151222.pdf

[xx] Tess Bennett 2024 'Social media giants "no longer fear reputation risks"' *AFR* https://www.afr.com/technology/social-media-giants-no-longer-fear-reputation-risks-20240422-p5flls

[xxi] eSafety Commissioner 2023 *eSafety demands answers from Twitter about how it's tackling online hate* https://www.esafety.gov.au/newsroom/media-releases/esafety-demands-answers-from-twitter-about-how-its-tackling-online-hate

[xxii] Attorney General's Department 2024 *Government response to the Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

[xxiii] European Commission 2024 *Commission opens formal proceedings against Meta* https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664

[xxiv] Mariam Cheik-Hussein 2020 '"Fake News" - ACCC, media industry respond to Google's open letter' *Ad News* https://www.adnews.com.au/news/fake-news-accc-media-industry-respond-to-google-s-open-letter

[xxv] Keach Hagey, Mike Cherney & Jeff Horwitz 2022 'Facebook Deliberately Caused Havoc in Australia to Influence New Law, Whistleblowers Say' *WSJ* https://www.wsj.com/articles/facebook-deliberately-caused-havoc-in-australia-to-influence-new-law-whistleblowers-say-11651768302

[xxvi] Reset.Tech Australia 2022 *How Meta extorted Australia* https://au.reset.tech/news/how-meta-extorted-australia/

[xxvii] Digi 2022 *Australian Code on Disinformation and Misinformation* https://digi.org.au/wp-content/uploads/2022/12/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-_-December-22-2022.docx.pdf

[xxviii] ABC News 2023 'Elon Musk's X reprimanded after disinformation safety feature scrapped' *ABC News* https://www.abc.net.au/news/2023-11-28/x-twitter-reprimanded-over-disinformation-safety-feature-removal/103158330

[xxix] Minister for Communications 2024 *Online Safety (Basic Online Safety Expectations) Amendment Determination 2024* https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-bose-amendment-determination-2024.pdf, Schedule 1 Amendments, 3, which states that 'if a service or a component of a service (such as an online app or game) is likely to be accessed by children (the children's service) – ensuring that the default privacy and safety settings of the children's service are robust and set to the most restrictive level'

[xxx] Commonwealth of Australia 2021 *Online Safety Act 2021* https://www.legislation.gov.au/C2021A00076/latest/text, which defines child as 'an individual who has not reached 18 years'

[xxxi] See Reset.Tech Australia 2024 *Submission to the Statutory Review of the Online Safety Act Issues Paper* https://au.reset.tech/news

[xxxii] Andrea Carson 2024 'Is Australia's golden age of third-party fact checking over?' *The Conversation* https://theconversation.com/is-australias-golden-age-of-third-party-fact-checking-over-224502

[xxxiii] John Storey 2023 'Biased "Fact Checkers" Show How Misinformation Laws Will Be A Disaster For Australia' *Institute of Public Affairs* https://ipa.org.au/publications-ipa/media-releases/biased-fact-checkers-show-how-misinformation-laws-will-be-a-disaster-for-australia#

[xxxiv] Ange Lavoipierre 2024 'Pro-Russian influence campaign targets Australian media outlets, including ABC, researchers find' *ABC* https://www.abc.net.au/news/2024-06-04/russia-war-ukraine-propaganda-disinformation-australian-media/103927386

[xxxv] Updated alert from CheckFirst and Reset.Tech. Available on request

[xxxvi] Meta 2024 *Where We Have Fact Checking* https://www.facebook.com/formedia/mjp/programs/third-party-fact-checking/partner-map

[xxxvii] Calculated from their publicly available list of 'fact checks', including 32 from the AFP, 32 from AAP and none from RMIT FactLab. (See AFP 2024 *AFP Australia* https://factcheck.afp.com/AFP-Australia; AAP 2024 *Factcheck* https://www.aap.com.au/factcheck/; RMIT FactLab 2024 *Debunks* https://www.rmit.edu.au/about/schools-colleges/media-and-communication/industry/factlab/debunking-misinformation)

[xxxviii] AAP 2024 *No, French have not imposed martial law in New Caledonia* https://www.aap.com.au/factcheck/no-french-have-not-imposed-martial-law-in-new-caledonia/

[xxxix] AFP Australia 2024 *Experts rubbish claim Greta Thunberg related to non-existent Rothschild* https://factcheck.afp.com/doc.afp.com.34QL3B3

[xl] See Reset.Tech Australia 2024 *Functioning or Failing* https://au.reset.tech/news/report-functioning-or-failing/

[xli] Reset.Tech Australia 2024 *Statement on our complaint against Meta* https://au.reset.tech/news/statement-on-our-complaint-against-meta/

[xlii] Reset.Tech Australia 2024 *Not Just Algorithms: Assuring User Safety Online With Systemic Regulatory Frameworks* https://au.reset.tech/news/report-not-just-algorithms/

[xliii] UK 2023 *Online Safety Act 2023* https://www.legislation.gov.uk/ukpga/2023/50/enacted

[xliv] Canada 2024 *Online Harms Bill 2024* https://www.parl.ca/LegisInfo/en/bill/44-1/c-63

[xlv] Rys Farthing & Lorna Woods 'The dangers of pluralisation: A singular duty of care in the Online Safety Act' *The Policymaker* https://thepolicymaker.jmi.org.au/the-dangers-of-pluralisation-a-singular-duty-of-care-in-the-online-safety-act/

[xlvi] EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[xlvii] Office of the eSafety Commission 2023 *Assessment tools* https://www.esafety.gov.au/industry/safety-by-design/assessment-tools

[xlviii] Sally Broughton & Micova Andrea Calef 2022 *Elements For Effective Systemic Risk Assessment Under The DSA* https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf

[xlix] EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[l] European Commission 2024 *Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act* https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2373

[li] Article 35, EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[lii] eSafety Commissioner 2024 *Responses to transparency notices* https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices

[liii] Commonwealth of Australia *Online Safety Act* 2021 Division 3(A) 59 2 https://www.legislation.gov.au/C2021A00076/latest/text

[liv] See, for example, *X Corp v eSafety Commissioner* (VID956/2023), status available at: https://www.comcourts.gov.au/file/Federal/P/VID956/2023/actions

[lv] See, for example, Reset.Tech Australia 2024 *Achieving digital platform public transparency in Australia* https://au.reset.tech/news/achieving-digital-platform-public-transparency-in-australia/

[lvi] See, for example, Reset.Tech Australia 2024 *Achieving digital platform public transparency in Australia* https://au.reset.tech/news/achieving-digital-platform-public-transparency-in-australia/

[lvii] Article 40, EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[lviii] EU 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj, Article 51(3)

[lix] UK Department for Science, Innovation & Technology 2024 *Online Safety Act: explainer* https://www.gov.uk/government/publications/online-safety-act-explainer/

[lx] For more information see UK 2024 *Online Safety Act: new criminal offences circular* https://www.gov.uk/government/publications/online-safety-act-new-criminal-offences-circular/online-safety-act-new-criminal-offences-circular

[lxi] Georgie Hewson 2023 'Australia's eSafety commission fines Elon Musk's X $610,500 for failing to meet anti-child abuse standards' *ABC* https://www.abc.net.au/news/202310-16/social-media-x-finedover-gaps-in-child-abuseprevention/102980590

[lxii] ACCC nd *Fines and penalties* https://www.accc.gov.au/business/compliance-and-enforcement/fines-and-penalties

[lxiii] ASIC 2023 *Fines and Penalties* https://asic.gov.au/about-asic/asic-investigations-and-enforcement/fines-and-penalties/

[lxiv] We commend the ACCC for its thoughtful and comprehensive inquiry into data brokers and data firms and encourage further scrutiny of these sectors: ACCC 2024 *Digital platform services inquiry interim report 8: data products and services – how information is collected and used by data firms in Australia* https://www.accc.gov.au/system/files/Digital-platform-services-inquiry-March-2024-interim-report.pdf

[lxv] Reset.Tech 2023 *Australians for Sale* https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf

[lxvi] Carly Kind 2024 'New laws needed to stop TikTok and other social media giants "harvesting" data' *The Australian* https://www.theaustralian.com.au/business/technology/new-laws-needed-to-stop-tiktok-and-other-social-media-giants-harvesting-data-privacy-commissioner-carly-kind/news-story/186676ee74ad7378d9a82b465a976cc5

[lxvii] ICCL 2023 *Europe's hidden security crisis* and *America's hidden security crisis* https://www.iccl.ie/2023/new-iccl-reports-reveal-serious-security-threat-to-the-eu-and-us/

[lxviii] Jon Keegan 2023 'Life 360 sued for selling location data' *The Markup* https://themarkup.org/privacy/2023/06/01/life360-sued-for-selling-location-data

[lxix] Human Rights Watch 2022 *How dare they peep into my private life* https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[lxx] Darren Davidson 2017 'Facebook targets "insecure" young people' *The Australian* https://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6

[lxxi] Attorney General's Department 2023 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[lxxii] ACMA 2024 *How to spot a scam* https://www.acma.gov.au/phone-and-sms-scams

[lxxiii] Reset.Tech 2023 *Australians for Sale* https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf

[lxxiv] Reset.Tech Australia 2023 *Is political content over- or under-moderated?* https://au.reset.tech/news/report-is-political-content-over-or-under-moderated/

[lxxv] ACCC 2024 *Digital platform services inquiry interim report 8: data products and services – how information is collected and used by data firms in Australia* https://www.accc.gov.au/system/files/Digital-platform-services-inquiry-March-2024-interim-report.pdf

[lxxvi] Attorney General's Department 2023 *Government response to the Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report