

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

regarding the

Inquiry into the influence and impacts of social media on Australian society

28 June 2024

Who we are

Digital Rights Watch is a charity organisation founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness and freedom. Digital Rights Watch educates, campaigns and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Samantha Floreani | Head of Policy |

General remarks

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Joint Select Committee on Social Media and Australian Society in relation to the inquiry into the influence and impacts of social media on Australian society.

As Australia's leading digital rights organisation, DRW is primarily concerned with the human rights, safety and wellbeing of individuals and communities in the digital age. **As always, we emphasise that privacy and digital security are essential to uphold safety.** Questions of legitimacy, proportionality, and reasonableness also must be carefully considered in any rights-balancing activity when determining tech policy interventions.

Digital Rights Watch actively participates in public consultations regarding the development of legislation and policy in relation to technology and human rights. We have consistently contributed to the public debate regarding many of the inquiry's terms of reference, in particular in relation to age verification and the news media bargaining code.

Our recent submissions relevant to this inquiry include:

- Submission to the [statutory review of the Online Safety Act](#) (June 2024)
- Submission to the Inquiry into the [influence of international digital platforms](#) (March 2023)
- Submission on the proposed *Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2023* (August 2023)
- Submission to the [Inquiry into Online Safety and Social Media](#) (January 2022)
- Submission on the [proposed News Media Bargaining Code](#) (January 2021)
- Submission on the [draft online safety Industry Codes](#) (October 2022) and the [subsequent draft Industry Standards](#) (January 2024)
- Submission in response to the Restricted Access Systems [discussion paper](#) (September 2021) and subsequent [draft declaration](#) (November 2021)

Digital Rights Watch welcomes the opportunity to participate in public hearings or further consultations and to provide comment and feedback on future specific proposals.

Human rights must be at the centre of Australia's approach to tech policy

Protecting, enhancing and upholding human rights is essential to ensuring Australia's technology policy is robust, fit for purpose, and meaningfully contributes to the improvement of individuals and community wellbeing both online and off.

It is often the case that there is significant complexity and nuance to be considered when determining the best approach to deal with online issues and harms. A human-rights

approach can help ensure that rights are appropriately balanced where there might be conflicts present. Very few rights are absolute, and so a human-rights approach assesses which rights might be interfered with, and then determine if it is necessary and proportionate interference, for a legitimate purpose.

In Australia and internationally, online safety policy proposals often threaten to infringe upon human rights, for instance by undermining end-to-end encryption (or mechanisms to side step it altogether), privacy-invasive methods for age verification, processes which reduce or threaten online anonymity, and the reliance on increased automated content moderation. This is made worse in Australia with a lack of a federal human rights charter.

It is our view that additional safeguards are necessary to ensure that tech policy interventions regarding the influence and impact of social media in Australia uphold fundamental human rights and supporting principles.

Digital Rights Watch strongly suggests that the Australian government prioritise the creation and enactment of a federal Human Rights Act. Doing so would:

- assist in the creation of a rights-respecting culture in Australia,
- ensure that human rights are proactively considered in any new legislation,
- create a powerful tool to challenge injustice, including where facilitated by technologies, and
- provide opportunities for people to take action and seek justice where their rights have been violated.

We also support the creation of a separate but complementary Charter of Digital Rights and Principles, which could specifically focus on the application of human rights to existing and emerging technologies.¹ For example, the European Union's Declaration on Digital Rights and Principles was designed to complement existing rights, and to provide guidance for the European Union and its member states as they pursue "human centric" and "sustainable" digital transformation.²

Given that Australian leaders and policymakers are interested in Australia being a world leader in technology policy, and is embarking on numerous digital transformation projects and concurrent tech-related regulatory efforts, a guiding set of overarching digital rights and principles would be useful to ensure that Australia's digital future is grounded in human rights, safety and dignity of all Australians.

¹ We suggest that this could be modelled on the European Union's Declaration of Digital Rights and Principles. For more detail see: Digital Rights Watch Submission to The Parliamentary Joint Committee on Human Rights regarding the Inquiry into Australia's Human Rights Framework, 29 June 2023. Available at: <https://digitalrightswatch.org.au/2023/07/11/efa-sub-human-rights/>

² European Digital Rights and Principles, *European Commission*.
<https://digital-strategy.ec.europa.eu/en/policies/digital-principles/>

Recommendations

1. Enact a comprehensive federal Human Rights Act.
2. Develop an Australian equivalent to the European Union's Declaration of Digital Rights and Principles.

Protecting privacy is crucial to mitigating online harms

It is our view that robust privacy protections play an essential role in ensuring both rights and safety in online environments, on both an individual and systemic level.

On an individual level, robust privacy protections can protect people from harms such as predatory targeted marketing³ and targeted extreme content and disinformation⁴, data breaches and identity theft, and other flow on effects related to the data broker market⁵. This is counterproductive to the goals of increasing online safety.

On a larger scale, we urge the Committee to focus upon exposing and challenging the structures that give rise to online harms, which we see not as a standalone problem, but as a symptom of data-extractive business models of digital platforms and advertisers that dominate our digital ecosystem. Protecting privacy is an essential component to meaningfully challenging these business models.

Many online harms stem from rampant and intrusive generation, collection and monetisation of personal data. As such, legislative efforts directed toward social media platforms that target a symptom (such as removal of content; fact-checking), can address aspects of the problem, but without further intervention, leave the broader structures unaddressed. Digital Rights Watch sees bold privacy law reform as a key way to target the problem at its source: the commercial access to and exploitation of personal information.

We note that the Privacy Act 1988 is currently under review. In our view, strong privacy reform that favours the rights of users over data extractive business models is central to the goals of enhancing online safety for all people. For too long, Australia's privacy laws

³ Foundation for Alcohol Research & Education, 'New research shows kids are targeted with alcohol, gambling and junk food ads online,' 4 June 2024, <https://fare.org.au/new-research-shows-kids-are-targeted-with-alcohol-gambling-and-junk-food-ads-online/>

⁴ Samantha Floreani and Lizzie O'Shea, 'We must target the root cause of misinformation. We cannot fact check our way out of this,' *The Guardian*, 16 April 2024, <https://www.theguardian.com/commentisfree/2024/apr/26/australia-government-misinformation-bill-social-media-x>

⁵ ACCC, 'Consumers lack visibility and choice over data collection practices,' 21 May 2024, <https://www.accc.gov.au/media-release/consumers-lack-visibility-and-choice-over-data-collection-practices>

have not adequately reflected public expectations, and the lack of enforceable personal privacy rights continues to be a glaring omission in the international context.

Recommendations

3. Prioritise robust reform to Australia's *Privacy Act*.
4. Implement greater restrictions on targeted advertising: prohibit targeted advertising from predatory industries, prohibit targeted advertising directed at children entirely.
5. Implement greater regulation of data brokers.

Age verification is not an appropriate method to protect Australian children from the harms of social media

We note the term of reference:

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

First, we wish to challenge the framing of this term of reference, which pre-supposes that any and all access to social media is something from which children must be protected. While we appreciate that there are many challenges and pitfalls of social media that warrant careful intervention, we caution the Committee against the temptation to portray social media as entirely good or bad—such a dichotomous view can not only lead to misguided policy outcomes, it is also inaccurate and counterproductive to meaningful online safety for children.

Research recently released from a health advisory body from the American Psychological Association on social media use in adolescence finds that “using social media is not inherently beneficial or harmful to young people.”⁶

While there has been much heated public discourse recently regarding the impact of social media upon children and young people, they themselves have been notably absent from the discussions.⁷ Research where teens are part of the discourse paints a nuanced

⁶ ‘Health advisory on social media in adolescence,’ *American Psychological Association*, accessed 25 June 2024,

<https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>

⁷ Samantha Floreani, ‘Australian politicians think 15-year-olds are old enough to go to jail but not go on Facebook. They’re kidding themselves,’ *The Guardian*, 23 May 2024,

<https://www.theguardian.com/commentisfree/article/2024/may/23/australia-social-media-ban-under-16-children-comment>

picture of adolescent online life, with a vast array of experiences and attitudes beyond an all-good or all-bad narrative.⁸

Research conducted by the Young and Resilient Research Centre – which prioritises meaningfully engaging with children – notes that while negative experiences on social media do occur, many young people see the online world as a safe haven.⁹ Even research by the eSafety commissioner – who is tasked with children's online safety – has noted that children's experiences online can be both positive and negative, and that a quarter of children who turn to the internet for support do so on social media.¹⁰ Recently, the eSafety Commissioner has publicly expressed concerns regarding the possible negative flow on effects of attempting to ban children from social media altogether.¹¹

Children and young people ought to be able to participate in modern life, much of which happens online. Attempts to ban children and young people from social media entirely or subject them to invasive biometric surveillance practices under the guise of “safety” would infringe upon a range of their rights, including freedom of expression, the right to privacy and the right to access information. Many young people rely on social media to forge identities, find communities, access support and express themselves.

Attention should be directed towards dismantling corporate surveillance and targeted advertising, which are detrimental to children's (and indeed everyone's) online safety and participation. A key way to do this is to challenge digital platforms' data-extractive business models through robust privacy reform, and to help foster the kind of economic structures that do not promote hyper-commercialism and the practices and values that go with it. We urge the Committee to take seriously the role that protecting privacy can play in enhancing the safety and wellbeing of children online.

The shortcomings of age assurance technology

Digital Rights Watch has long raised concerns regarding the use of age assurance technology—including both age verification and age estimation—to restrict access to

⁸ Monica Anderson, Emily A. Vogels, Andrew Perrin and Lee Rainie, 'Connection, Creativity and Drama: Teen Life on Social Media in 2022,' *Pew Research Centre*, 16 November 2022, <https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/>

⁹ Linda Marsden, Lilly Moody, Betty Nguyen, Lilly Tatam, Louisa Welland, Professor Amanda Third, 'Reimagining online safety education through the eyes of young people: co-design workshops with young people to inform digital learning experiences,' *Young & Resilient Research Centre*, 2022, https://www.westernsydney.edu.au/_data/assets/pdf_file/0004/1976503/Reimagining_Online_Safety_Education.pdf

¹⁰ eSafety Commissioner, 'Mind the Gap,' February 2022, <https://www.esafety.gov.au/research/mind-gap>

¹¹ Josh Taylor, 'Social media age restrictions may push children online in secret, Australian eSafety commissioner says,' *The Guardian*, 23 June 2024, <https://www.theguardian.com/australia-news/article/2024/jun/23/social-media-age-restrictions-may-push-children-online-in-secret-australia-regulator-says>

particular content such as online pornography, or entire digital platforms or online services.

Our core concerns are summarised as follows:

- (1) age verification creates significant privacy and digital security risks that represent a disproportionate human rights infringement when balanced against the purported benefits;
- (2) age verification systems and programs have significant problems of implementation and workability, including issues of bias, accuracy and the ability to easily bypass systems by way of a VPN, or manipulate some age estimation tools with ageing filters.

Age verification is rife with significant privacy and digital security risks, as well as critical effectiveness and implementation issues. Age verification is privacy-invasive, which undermines the objective of reducing online harm. Most forms of age verification require the provision of additional personal information to be effective. Incentivising companies, third parties, and government agencies to collect, use and store additional personal information to conduct age verification creates additional privacy and security risk, which in turn can exacerbate online harms.

Recent research into age estimation tools—that is, tools that attempt to estimate or infer a user's age based on data inputs such as biometrics by way of a facial scan—shows that such technologies are unreliable, and have a racial and gender bias.¹² Other research has investigated the use of age estimation video surveillance in gambling establishments. When the developers of the age estimation tool were interviewed they admitted that it was of limited efficacy in detecting people under the age of 18. Researchers found that the age estimation tool was “performative in nature”, ultimately relying upon humans to do the actual work of age verification.¹³ Recent reporting has also documented the ease with which it is possible to bypass such tools.¹⁴ In the eSafety Commissioner's own research from 2023, young people expressed concern regarding age assurance's limited efficacy, as well as privacy and security issues.¹⁵

We've had this debate before

Digital Rights Watch was pleased to see the sensible decision from the Australian government not to move ahead with the trial for age verification for online pornography in

¹² Stardust, Z., Obeid, A., McKee, A., & Angus, D. (2024). [Mandatory age verification for pornography access: Why it can't and won't 'save the children'](https://doi.org/10.1177/20539517241252129). *Big Data & Society*, 11(2). <https://doi.org/10.1177/20539517241252129>

¹³ O'Neill, C., Selwyn, N., Smith, G., Andrejevic, M., & Gu, X. (2022). [The two faces of the child in facial recognition industry discourse: biometric capture between innocence and recalcitrance](https://doi.org/10.1080/1369118X.2022.2044501). *Information, Communication & Society*, 25(6), 752–767. <https://doi.org/10.1080/1369118X.2022.2044501>

¹⁴ Cam Wilson, 'I tricked a selfie AI age-verification demo into letting a child 'buy' a knife,' *Crikey*, 14 June 2024, <https://www.crikey.com.au/2024/06/14/selfie-ai-age-verification-tool-filter-trick/>

¹⁵ eSafety Commissioner, 'Questions, doubts and hopes: Young people's attitudes towards age assurance and the age-based restriction of access to online pornography,' September 2023, <https://www.esafety.gov.au/sites/default/files/2023-08/Questions-Doubts-and-Hopes.pdf>

August 2023.¹⁶ This decision was based on immaturity of the technology, privacy, digital security and implementation issues. However, this decision was later reversed in response to pressure to act on increased misogyny and violence against women.¹⁷

Using a human rights approach, the privacy invasion that comes with age verification may be justified, if it is a reasonable, necessary and proportionate means for a legitimate purpose.¹⁸ However, to date, there is no compelling evidence that this is the case.

First, many young people access adult content on social media sites, rather than dedicated pornography sites. Mandating age assurance technology misses the mark, and to extend the proposal to apply to all social media sites would be a serious overreach. Further, the research is complex and at times conflicting when it comes to connecting mainstream pornography with gender-based violence.¹⁹ Making policy decisions that impact human rights based on assumptions and unclear evidence about harm is not appropriate.

Second, in 2021 the Coalition government drafted the *Online Privacy Bill*, which would have required platforms to verify the age of their users and obtain parental consent for those under the age of 16.²⁰ Research conducted afterwards found that parents and carers were initially enthusiastic about the prospect of stronger laws to help protect their children, but this quickly deflated when they learned of the measures that would be needed to actually enforce it, such as providing identity documents to platforms or third parties, increased app tracking and monitoring, and ongoing age verification processes such as face scans.²¹

¹⁶ Australian Government, 'Australian Government response to the Roadmap for Age Verification,' *Department of Infrastructure, Transport, Regional Development, Communications and the Arts*, 30 August 2023, <https://www.infrastructure.gov.au/department/media/publications/australian-government-response-roadmap-age-verification>

¹⁷ Prime Minister of Australia, 'Tackling online harms,' Media Release, 1 May 2024, <https://www.pm.gov.au/media/tackling-online-harms>

¹⁸ Lizzie O'Shea, 'Let's get this right and avoid knee-jerk decisions on misogyny and men's violence against women,' *Crikey*, 2 May 2024, <https://www.crikey.com.au/2024/05/02/misogyny-violence-against-women-pornography-privacy-age-restriction/>

¹⁹ Lim, M.S.C., Carrotte, E.R. & Hellard, M.E. (2016). The impact of pornography on gender-based violence, sexual health and well-being: what do we know? *Journal of Epidemiol Community Health*, 70, 3-5. Mestre-Bach, G., Villena-Moya, A., & Chiclana-Actis, C. (2024). Pornography Use and Violence: A Systematic Review of the Last 20 Years. *Trauma, Violence, & Abuse*, 25(2), 1088-1112. <https://doi.org/10.1177/15248380231173619>.

²⁰ Australian Government, 'Online Privacy Bill Exposure Draft,' Attorney-General's Department, 25 October 2021, <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>

²¹ University of Sydney, 'New study reveals teenagers' social media use and safety concerns,' 6 October 2023, <https://www.sydney.edu.au/arts/news-and-events/news/2023/10/06/new-study-reveals-teenagers-social-media-use-and-safety-concerns.html>

These issues with age verification make it an unviable mechanism and we argue it should not be mandatory on social media platforms or online pornography websites. Further investment in prevention of gendered violence should address systemic misogyny embedded in society, which has been well-established by decades of research.

Recommendation

6. Do not create requirements for mandatory age verification for social media, nor attempt to blanket-ban children under 16 from accessing social media platforms.

The News Media Bargaining Code was never the appropriate mechanism to safeguard journalism in Australia

With regard to the term of reference:

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

We note that Meta has not *abandoned* the deals, rather, the existing agreements with news companies have concluded, and Meta has chosen to not establish new agreements. The company is entitled to do this under the News Media Bargaining Code ('Bargaining Code'). This is an important distinction to understand the realistic context and shortcomings of the Bargaining Code.

Under the currently established Bargaining Code, the government is able to respond by deciding to designate Meta, which would force negotiations between Meta and Australian news media companies and could lead to a binding arbitration process. Given the public-facing statements made by Meta²² and their decision to remove news from Facebook in Canada²³ following the passage of the *Online News Act* (which was inspired

²² Facebook, 'An Update on Facebook News,' *Meta*, 29 February 2024, <https://about.fb.com/news/2024/02/update-on-facebook-news-us-australia/>

²³ Following the passage of the *Online News Act* which was inspired by Australia's News Media Bargaining Code and promised "fairness in the Canadian digital-news marketplace", Facebook blocked news on their platform in Canada. See: 'Changes to News Availability on Our Platforms in Canada,' *Facebook*, 1 June 2023, <https://about.fb.com/news/2023/06/changes-to-news-availability-on-our-platforms-in-canada/>

Note also that the decision to block news links in Canada resulted in almost no reduction in Canadian's use of Facebook. See Katie Paul and Steve Scherer, 'Exclusive: Meta's Canada news ban fails to dent Facebook usage,' *Reuters*, 29 August 2023

by the Bargaining Code in Australia), the likely outcome of attempts to force arbitration is that Meta may choose to remove news from Facebook entirely.

Digital Rights Watch has long been critical of the approach of the Bargaining Code, as it further tethers Australian journalism to the profits and whims of digital platforms. In doing so, it entrenches curatorial opacity (by way of engagement and amplification algorithms) and data-extractive business models based on surveillance capitalism and behavioural advertising.

In September 2021, we expressed concern that while the Bargaining Code may have addressed part of the media sector's *economic* problems, it exacerbated its *societal* ones, including the increasing dominance of false and sensationally polarising content.²⁴ This is because the animating force behind how platforms organise content is their business model, which works by keeping people on-platform for as long as possible, so that more data can be generated for the purpose of targeted advertising. It follows that content that elicits an emotional or sensational response — and therefore keeps people online for longer — performs well on commercial platforms. There is research linking behavioural advertising with the spread of misinformation online.²⁵

This is the system that Australian news media outlets must become reliant upon under the Bargaining Code to shore up their economic model. Such a distribution mechanism works better for some news organisations than others, such as Sky News, which has been successful at exploiting this attention-driven model and spreading misinformation.²⁶ Subjecting the bulk of the Australian news ecosystem to reliance on overseas commercial platforms promises to reduce diversity and under-serve civic and democratic values.

Research conducted on the Bargaining Code shows that while it had some success, there were problems in its actual operation, including significant information asymmetries between news media outlets and platforms in the process of negotiation, as well as providing a significant competitive advantage to news organisations able to secure deals with digital platforms over those who could not.²⁷

In August 2020 we noted in our submission that we had serious concerns regarding the impact the Bargaining Code would have upon smaller, independent and regional news

<https://www.reuters.com/technology/metas-canada-news-ban-fails-dent-facebook-usage-2023-08-29/>

²⁴ Lizzie O'Shea and Mark Andrejevic, 'The misinformation engine,' *Overland*, 1 September 2021, <https://overland.org.au/2021/09/the-misinformation-engine/>

²⁵ Karen Hao, 'How Facebook and Google fund global misinformation' *MIT Technology Review*, 20 November 2021, <https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/?s=0>

²⁶ Hurcombe, E., & Meese, J. (2022). Australia's DIGI Code: what can we learn from the EU experience? *Australian Journal of Political Science*, 57(3), 297–307. <https://doi.org/10.1080/10361146.2022.2122774>

²⁷ Bossio, D., Carson, A., & Meese, J. (2024). [A different playbook for the same outcome? Examining Google's and Meta's strategic responses to Australia's News Media Bargaining Code](#). *New Media & Society*, 0(0). <https://doi.org/10.1177/14614448241232296>

outlets. While some regional news media companies did secure funds by way of the Bargaining Code, it was only a tiny fraction of the regional and rural newspapers across Australia.²⁸ The experience in Canada has shown that smaller news providers have been significantly more impacted by Meta's decision to remove news than the bigger players, as they have a higher reliance on large platforms like Facebook.²⁹

Digital Rights Watch encourages the committee to think carefully regarding the extent to which Australia wants to tie the long-term sustainability of Australian journalism to commercial digital platforms, namely companies like Meta, which have shown little interest in supporting the news sector or indeed with regard to the distribution of quality content.

In our view, the Bargaining Code exposes a failure of imagination on the part of policy makers. It is clear that action is needed to support news and journalism in the face of the reconfigured business environment, but we urge the Committee to think beyond Google, Facebook and other Silicon Valley tech giants. **Relying on these companies' model of surveillance capitalism is unlikely to serve Australia's interests in the long run.**

If we are interested in a robust media sector to underpin Australia democracy, it would be more beneficial to turn to funding mechanisms that minimise the role played by advertising, rather than making vital news media more reliant on the invasive and largely unaccountable model of data-driven ad targeting.

Challenging the underlying business models of digital platforms is essential to combat online mis and disinformation

With regard to the terms of reference:

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

and

(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;

We note that while Australian journalism can play an important role in countering mis- and disinformation on digital platforms, there are also many news outlets that actively contribute to the creation and dissemination of sensationalist, misleading and divisive

²⁸ The University of Canberra News and Media Research Centre, McCallum, K, Park, S., Fisher, C., McGuinness, K. (2022). Submission to the House of Representatives Standing Committee on Communications and the Arts: Inquiry into Australia's regional newspapers, page 18.

²⁹ Jay Heisler, 'Facebook News Ban in Canada Leaves Small Outlets Struggling,' *Voice of America*, 15 February 2024, <https://www.voanews.com/a/facebook-news-ban-in-canada-leaves-small-outlets-struggling-/7489564.html>

material. It is essential that in Australia's endeavours to combat the harms of online mis- and disinformation that the media sector be rigorously examined as part of both the problem and the solution. Misinformation has never simply been a social media problem: it is inextricably connected to problems in traditional broadcast (mainstream) media.

Further, news outlets in Australia increasingly rely upon social media and digital platforms as tools to build audiences and distribute content. This reliance is exacerbated by the News Media Bargaining Code, which rather than challenging the reliance of Australian journalism on digital platforms, further entrenches it.

Online mis- and disinformation has been widely recognised as detrimental to democracy. Left unchecked, it threatens every pathway to a fairer and more sustainable Australia.

Solutions in Australia have largely focused on surface-level interventions such as content removal and fact-checking. These approaches are well-intentioned and useful, but they cannot be scaled to meet the problem at hand. They cannot respond to the industrial levels of low quality and polarising content that pollute our information ecosystem. This compromises the quality of public debates and the functioning of our democracy.

For example, social media platforms reward content that keeps people on their platforms for as long as possible. This is because the more time that a person spends on a platform, the more data can be collected about them, and in-turn increases the opportunities platforms can offer to advertisers to sell targeted ads.

Polarising, extreme or controversial material performs well on these metrics, meaning that such content gets boosted by engagement and amplification algorithms. This is made worse by content recommendation systems that take people down algorithmic 'rabbitholes'³⁰ and revenue sharing schemes that create direct financial incentives for content creators to create and share content that is highly engaging and tailored for virality. Consider for instance that some people with a Premium X account made money sharing both Islamophobic and anti-Semitic misinformation immediately following the Bondi Junction attack in Sydney.³¹ It is antithetical to the role played by news outlets in a democratic society to make them reliant on distribution platforms that have no commitment to the norms and standards of journalism.

Research has indicated that mis- and disinformation is less effective at changing people's beliefs or voting practices than often imagined, but *is* effective at entrenching and

³⁰ An algorithmic rabbithole refers to the experience of being highly engaged on a digital platform and being recommended content that is similar to material you have already engaged with, usually increasing in extremity and frequency the further you go. A common example is TikTok's algorithm which is particularly adept at this process. For an explanation we recommend this video: <https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796>

³¹ Ariel Bogle, 'False claims started spreading about the Bondi Junction stabbing attack as soon as it happened,' *The Guardian*, 15 April 2024, <https://www.theguardian.com/australia-news/2024/apr/15/false-claims-started-spreading-about-the-bondi-junction-stabbing-attack-as-soon-as-it-happened>

enhancing pre-existing beliefs.³² Many digital platforms hold user attention by showing them content that is similar to that in which they have already shown an interest, therefore the very design of engagement algorithms threatens to exacerbate the potential confirmation-bias of online mis- and disinformation.

The impact of personalised disinformation campaigns is likely to be exacerbated in the future by developments in generative AI, which promises to deliver increasingly granular forms of content customization at scale.

In short, data-extractive and surveillance-based business models harm our democracy. They function to undermine our capacity to empathise and compromise across social, political and cultural divides, which are essential features of a functioning democracy. Collective concerns such as the public interest, human rights, community responsibility and upholding democracy struggle to compete with the profit motive, and in practice are not prioritised by commercial social media platforms.

The throughline of the systems described above, including generative AI, is that they *rely* upon access to massive amounts of personal information in order to function. We strongly urge the committee to consider that at the heart of most issues related to the impacts of commercial social media platforms upon Australian society are ultimately *data problems*, and any meaningful intervention must consider, and ultimately challenge, the rampant generation, collection, and commodification of personal data for profit.

Recommendation

7. Ensure that approaches to combat online mis- and disinformation meaningfully grapple with the underlying business models of digital platforms which make mis- and disinformation so prevalent and powerful.

³² Magda Osman, 'Disinformation is often blamed for swaying elections – the research says something else,' *The Conversation*, 27 January 2024, <https://theconversation.com/disinformation-is-often-blamed-for-swaying-elections-the-research-says-something-else-221579>