THE UNIVERSITY OF MELBOURNE

24 February 2023

Addressing Big Tech Regulation in Australia

Response to Senate Inquiry Into International Digital Platforms Operated by Big Tech Companies

The School of Computing and Information Systems and the Centre for AI and Digital Ethics welcome this opportunity to contribute to the *Senate Inquiry into International Digital Platforms*.

Digital platforms play an increasing role in Australian public and private life–they are gatekeepers that control our access to goods, information, and services. However, *with great power comes great responsibility*[1] and as numerous international governmental and non-governmental bodies have found, platforms are failing to adequately manage their share of the burden.

The Senate's inquiry is therefore a prudent measure that we hope is accompanied by appropriate regulatory action, to improve the Australian platform landscape.

Executive Summary Recommendations

Algorithmic Transparency

- We support the call in the issues paper to enhance the ACCC's investigative capacity by expanding in-house technical and data science expertise, to better discharge its regulatory duties.

Privacy Breaches

- We are in favour of regulation that includes government levied penalties, which will in turn empower Chief Information Security Officers (CISOs) to protect their organisations by increasing their access to key decision makers within their organisation.
- We contend that increased penalties will also act as a disincentive against collecting unnecessary amounts of personal data.
    - We note however that unduly harsh penalties may have adverse effects such as causing organisations to cover up privacy breaches. We therefore recommend penalties be calibrated via consultation that includes industry voices.

Data and Privacy

- In line with our recommendations to the ongoing *Privacy Act Review,* we recommend:

[1] Stan Lee, *Amazing Fantasy #15* (Marvel Comics, 1962).

  - We argue that notice and consent regimes are insufficient to address privacy harms. We instead advocate for a regime that requires platforms to adhere to pro-privacy practices.
  - We support regimes to allows individuals to correct errors in their collected information, withdraw consent for process, and to mandate subsequent erasure.
  - We support standardised and simple consent on-boarding, with standard iconographs and layouts, to help minimise consumer consent fatigue.
  - We support amendments to 52(1)(b)(ii) and 52(1A)(c) of the privacy act that requires APP covered entities to both identify and mitigate both actual and foreseeable losses.
  - We support the introduction of a Federal Privacy Ombudsman as an accessible and effective way for individuals to vindicate their rights.
  - We argue that reintroducing the *Privacy Amendment (Re-identification) Offence Bill 2016* inappropriately targets those who identify issues, rather than those who caused them. Our research indicates that the act of reidentification is not the root of the issue–it is poor deidentification and release of data in the first instance.
- We recommend the ongoing review of whistleblower laws consider protection for whistle-blowers in Big Tech too.

Child Protection

- We argue that eSafety's intention to "expand to other acute harms" should not be allowed to dilute their focus on child protection, especially where this may impose weaken Australians' civil liberties or inadvertently pushing harmful actors away from where they are easily policed.
- We recommend against steps that overly expose platforms to civil liability for failures to remove user generated content, as experience in the US resulted in adverse outcomes.
- We recommend against adopting laws and regulations (such as those proposed or enacted under the previous government) that weaken security and privacy by decreasing the adoption of end-to-end encryption or other on-device privacy guarantees.

The Metaverse

- We warn that a Metaverse may prove to be a significant future source of fraudulent activity and scams. We recommend that regulators (in particular, the ACCC) should take a proactive approach to a) policing violations of existing consumer protection law and b) protecting competition as firms explore virtual reality offerings, rather than deferring to platform self-governance.

Cryptocurrency

- We recommend that cryptocurrency investments and investments in blockchain projects be restricted to sophisticated investors, where such investments have not met a bar similar[2] to those faced by ordinary issuers of securities, to avoid the proliferation of scams and fraudulent activity that current characterises the market for these digital assets.

[2] We note that narrowly tailored rules for crypto-securities may differ in specifics to those for ordinary securities. We merely assert that there should be a similar level of disclosure and legal stability.

Big Tech

- We recommend the introduction of new consumer protection laws to prohibit unfair trading practices, and the enhancement of merger and competition laws to address the systematic and well-documented harmful and anticompetitive business practices of Big Tech companies.
- We support the introduction of mandatory reporting and disclosure laws for Big Tech companies, protections for public interest research, and enhancements to regulator's analytical and investigative capacities, to combat the spread of mis- and dis-information on digital platforms.

Algorithmic Transparency

Question 2. Are there useful ideas in the proposed US legislation that are applicable in Australia?

The Australian Competition and Consumer Commission (ACCC) already plays a substantially similar role to the U.S. Federal Trade Commission (FTC). However, we support the call in the issues paper to better equip the ACCC to handle digital platform regulation. We refer you to our submission to the Treasury inquiry[3] where we argue that the ACCC should be equipped with expanded technical research and data science capabilities. We highlight the FTC's recent announcement of an Office of Technology which will hire individuals with backgrounds in technology to augment the FTC's consumer protection and antitrust missions. We advocate for a similar expansion of capabilities at the ACCC and support the parallel appointment of a Chief Technologist.

Privacy Breaches

Question 2: Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the scope and size of any such penalties?

We are in favour of regulation that includes government levied penalties, to help empower Chief Information Security Officers (CISOs) to protect their organisations. Stronger penalties increase the likelihood that a CISO can get access to decision-makers with budget-assigning powers (particularly the Board) and helps a CISO to make the for diverting funds

---

[3] Centre for Artificial Intelligence and Digital Ethics, Submission to Department of Treasury, *Digital Platforms Inquiry – Consultation on Regulatory Reform* (14 February 2023) 17 - 18, available at: <https://www.unimelb.edu.au/__data/assets/pdf_file/0008/4504634/Strengthing-Australian-Consumer-Protection-in-the-era-of-Digital-Platforms-14-Feb-23.pdf>.

to improving cyber security. This is justifiable as organisational failures in cybersecurity impose substantial *financial and non-financial* externalities on ordinary Australian who suffer privacy loss, identity theft, and financial fraud as the result of hacks.

Under current regimes a board may be reluctant to make an expensive investment in cybersecurity upgrades because information security may be seen as a cost centre, not a revenue centre, for the organisation. Even the best in-house information security or privacy staff may face an uphill battle in this regard. Thus, providing organisational incentive to avoid stricter penalties, within reason, may help.

Penalties act as a deterrent against excessive data collection, and against keeping collected data for longer than necessary. One approach that should be considered is to structure penalties not against the size of an organisation, but against the amount of sensitive information that an organisation holds. That is, organisations that hold more sensitive information should be subjected to larger penalties, regardless of the organisation's size. Doing so could create a powerful incentive for smaller and medium sized organisations (who generally have fewer resources to devote to cyber security and data protection) to avoid collecting and storing too much sensitive information.

However, there may be diminishing returns thus extreme penalties may be no additional help and may simply be viewed as unduly harsh. Further, such unreasonably harsh penalties may incentivise organisations or staff to hide problems rather than dealing with them openly, thus weakening the response capability. Thus, we recommend calibrating the level penalties through public consultation that includes industry voices.

Data and Privacy

Question 2: Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the scope and size of any such penalties?

We suggest the government consider scaling any penalties not according to the size of an organisation but by the amount of sensitive information an organisation holds. This would disincentivise over-collection and incentivise deleting sensitive information when it is no longer necessary to store.

Question 3: Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?

Significant changes are needed to Australia's privacy laws to address developments since the introduction of the Privacy Act in 1988, in particular the increased storage and processing of Australian data by a wide variety of digital platforms (domestic and international).

The Attorney General is currently conducting a comprehensive inquiry into the Privacy Act, with a view to law reform necessary to better protect Australians. The Centre for AI and

Digital Ethics has contributed two submissions[4] to the inquiry and we reiterate here our recommendations most relevant to large digital platforms and refer readers to the Attorney General's inquiry and our submissions for detailed argumentation.

- We argue that notice and consent regimes are insufficient to address privacy harms as individuals cannot be meaningfully expected to spend the large amount of time necessary to analyse and ruminate over consent for each service for which they engage. Consent is often a fiction. Therefore, we advocate for a regime that requires platforms to adhere to pro-privacy.
- We support regimes to allows individuals to correct errors in their collected information, withdraw consent for process, and to mandate subsequent erasure. There are additional safeguards that protect consumers despite the illusory nature of online consent.
- We support standardised and simple consent on-boarding, with standard iconographs and layouts, to help minimise consumer consent fatigue.
- We support amendments to 52(1)(b)(ii) and 52(1A)(c) of the privacy act that requires APP covered entities to both identify and mitigate both actual and foreseeable losses.
- We support the introduction of a Federal Privacy Ombudsman as an accessible and effective way for individuals to vindicate their rights.
- We argue that reintroducing the *Privacy Amendment (Re-identification) Offence Bill 2016* inappropriately targets those who identify issues, rather than those who caused them. Our research indicates that the act of reidentification is not the root of the issue–it is poor deidentification and release of data in the first instance.

We also recommend that whistleblower protections be expanded to ensure that individuals can safely come forward to identity security and privacy risks when firms fail to protect consumers. The last few years have illustrated the necessity of strong whistleblower protections[5], both through poor practices that came to light through whistleblowers and those that became clear only after it was too late.

As the Australian Commonwealth Attorney General has already flagged an overhaul of federal whistleblower protection laws[6] we recommend that such planned law reform consider ways to improve protections for whistleblowers in big tech.

---

[4] Centre for AI and Digital Ethics and Melbourne Law School, Submission to Attorney General's Department, *Review of the Privacy Act 1998 issues paper* (November 2020); Centre for AI and Digital Ethics, Submission to Attorney General's Department, *Review of the Privacy Act 1998 discussion paper* (24 January 2022).

[5] Philip Di Salvo, 'Leaking black boxes: Whistleblowing and big tech invisibility' (2022) 27(12) *First Monday*. https://firstmonday.org/ojs/index.php/fm/article/download/12670/10751

[6] Catie McLeod and Ellen Ramsley, 'Attorney General flag overhaul of Australia's whistle-blower protection laws' *News.com.au*, (23 November 2022) <https://www.news.com.au/national/politics/helen-haines-david-pocock-to-launch-whistleblower-report/news-story/706afaa7e39b5935777e9eeed396d821>.

Child Protection

Questions 1 and 2: How effective is the current legislative framework in protecting children and preventing online harm from occurring, and what more can be done to enhance online safety for child protection in Australia?

Australia currently leads the way in information-gathering and reporting steps related to child safety. Under section 56(2) of the *Online Safety Act 2021* (Cth), eSafety has the power to issue 'transparency notices' that compel online service-providers to report on the steps that they have taken to implement the Basic Online Safety Expectations. eSafety is empowered to publish questions and outline summaries of responses. That information is already being used by regulatory bodies across the world to improve accountability. For Australia, that work includes the ability to issue statements of non-compliance, in the context of a broader set of investigatory and compliance powers. These powers have paved the way for a better-informed approach to online safety for child protection, and it is our view that the scrutiny and implementation of sufficiently robust industry codes, including the imposition of civil penalties for failures to comply, will be a key aspect of an appropriate and proportionate response to serious harms.

We argue that eSafety's intention to "expand to other acute harms" should not be allowed to dilute their focus on child protection, especially where this may impose weaken Australians' civil liberties or inadvertently pushing harmful actors away from where they are easily policed.

We recommend against steps that overly expose platforms to civil liability for failures to remove user generated content. In the United States, the passage of the FOSTA-SESTA package forced platforms to choose between a) closing down, b) not moderating any content at all, or c) censoring legal content to avoid accidentally leaving illegal content online.[7] The premise was that by exposing platforms to civil liability and weakening safe harbours, platforms would more proactively police user-generated content, and that children would be better protected. However, the legislation was ineffective at its goals (as traffickers fragmented their activity to small platforms outside the reach of law enforcement) and resulted in censorship of LGBT+ and other vulnerable communities online[8].

Likewise, we recommend against rules (such as those proposed or enacted under the previous government[9]) that weaken security by decreasing the prevalence of security and privacy technologies such as end-to-end encryption. Proposed legislation in the UK and in

[7] Tom Jackman, 'House passes anti-online sex trafficking bill, allows targeting of websites like Backpage.com' *The Washington Post* (27 February 2018)
[8] Alexander Cheves, 'The Dangerous Trend of LGBTQ+ Censorship on the Internet' *Out* (6 December 2018) <https://www.out.com/out-exclusives/2018/12/06/dangerous-trend-lgbtq-censorship-internet>.
[9] See eg Carnegie Endowment for International Peace, *The Encryption Debate in Australia* (Briefing Paper, May 2019); *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).

the USA has sought to restrict such technologies and has rightfully been met with alarm by computer scientists and civil liberties organisations. Our research suggests that weakening encryption results in severe degradation in cybersecurity across sectors[10], imposes substantial privacy harms on regular individuals, and does little to stymie criminals who will shift to platforms outside the easy reach of the law.

The Metaverse

Question 1: Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better about how it will function?

We recommend that regulators (in particular, the ACCC) should take a proactive approach to a) policing violations of existing consumer protection law and b) protecting competition as firms explore virtual reality offerings. The mystique of new technology and ambiguity around regulation exposes Australians to scams and fraud–much as what happened with cryptocurrencies and NFTs. *Virtual investment property* offers another easy backstory for scammers to tell their marks.[11] However, because virtual reality products show genuine potential to become pervasive in civic life, it is critical that regulators ensure that competition concerns are adequately policed and that we learn the last decade's lesson on limits of platform self-governance.

Consumer Protection

The Australian government should expect a wave of fraud related to virtual investment property schemes because of the similarities with the cryptocurrency market. The Australian Competition and Consumer Commission's report on Scam Activity stated that cryptocurrency investment scams were the "main driver" of the sharp 35% increase in investment scam losses in 2021 from the previous year, with Australians reporting $99 million lost to these scams.[12] Given the growing interest in virtual reality, it is likely that similar fraudulent activities will occur in this market, posing a significant risk to Australian investors.

We therefore support the Australian government taking a proactive approach to policing activities such as fraud, by relying on the existing provisions of the ACL[13] *before* it has the deleterious impact that scams did with respect to cryptocurrencies.

---

[10] Shaanan Natanel Cohney, 'Too Important to Leave to Chance: Pseudorandom Number Generator Standardization & Security' (PhD Thesis, University of Pennsylvania, 2019).
[11] Carly Wanna, 'The once-Hot Market for Metaverse Land is Attracting Risky Bets' *Bloomberg* (19 October 2022) <https://www.bloomberg.com/news/articles/2022-10-18/decentraland-sandbox-virtual-land-in-metaverse-is-cheap-and-very-risky>.
[12] ACCC, 'Targeting scams; report of the ACCC on scams activity 2021' (Report, 4 July 2022) 11.
[13] Principally the prohibition on misleading and deceptive conduct (*Competition and Consumer Act 2010* (Cth) sch 2, s 18 ('*ACL*')), in similar fashion to current proceedings against Meta for scam advertisements on the platform: *Australian Competition and Consumer Commission v Meta* (Federal Court of Australia, NSD188/2022, commenced 18 March 2022).

Competition

A Metaverse poses even greater threats to social welfare down the line, some of which can be mitigated by present policy action. A Metaverse may someday serve similar "town-square" function in society to what we have seen with social media and should be regarded from the outset equipped with the benefit of hindsight regarding the dangers such technology.

We turn briefly to consider Meta's (formerly Facebook) role in the ecosystem–as the market leader. Though VR headset sales have flattened[14] and the "folk wisdom" media narrative is that this was temporary hype that will soon fade,[15] the potential benefits of improved VR suggest that Facebook's "Meta" pivot may nonetheless pan out.[16] The potential upsides to VR[17] make it the more necessary to ensure that Meta and other tech giants cannot suffocate the industry with anti-competitive behaviours.

Meta has the resources and foresight to ensure that they retain ownership and control of the ecosystem from top to bottom as it evolves. The company has already begun engaging in the same *acquire-copy-kill* strategy it employed to dominate the social media market as Facebook.[18] This involves stifling competition by alternately *acquiring competitors*[19]*, copying their product ideas*[20]*,* or using anticompetitive tactics to *kill* competitors entirely[21].

---

[14] 'VR Headset Sales Underperform Expectations, What Does It Mean For The Metaverse In 2023?' *Forbes* 6 January 2023).

[15] Ryan Mac, Sheera Krenkel and Kevin Roose 'Skepticism, confusion, frustration: Inside Mark Zuckerberg's metaverse struggles' *The New York Times* (9 October 2022).

[16] Trends towards hybrid-work may prove a particularly strong use-case for VR, which can offer a stronger sense of co-presence.

[17] Including expanded possibilities for interactive learning environments, mental health aids, and reduced carbon footprint from unnecessary travel.

[18] Shirin Ghaffary and Sara Morrison, 'Can Facebook monopolize the metaverse?' *Vox* (16 February 2022) <https://www.vox.com/recode/22933851/meta-facebook-metaverse-antitrust-regulation>.

[19] With their initial $2 billion buyout of Oculus VR in 2014, the company secured control of the IP and workers responsible for the most promising VR hardware, and now claim about 90% of the rapidly growing market for VR headsets (Michael Shirer, Jitesh Ubrani and Tom Mainelli 'Meta's Dominance in the VR Market will be Challenged in the Coming Years, According to IDC' *IDC* (Blog Post, 30 June 2022) <https://www.idc.com/getdoc.jsp?containerId=prUS49422922>. The company has since spent billions of dollars acquire at least 14 more VR-related companies. <https://www.ftc.gov/legal-library/browse/cases-proceedings/221-0040-meta-platforms-incmark-zuckerbergwithin-unlimited-ftc-v>

[20] Meta has been accused of copying popular programs in the app store including YUR Fit (with Oculus Move) and Rec Room (Oculus Horizon). While initially consumers benefit from optionality and competition, Meta's misuse of its market advantage can hinder new-entrants ability to fairly compete. (Naomi Nix, 'VR developers accuse Facebook of withholding the keys to metaverse success' *The Washington Post* (14 September 2022))

[21] Meta has made it difficult to load apps onto market-dominant hardware any other way than using their own native App store. They therefore control what apps get promoted and have been accused by app developers of failing to provide a clear path to full inclusion in their store. The app store also takes a 30% cut of all sales on the app store, leading to a conflict of interest (paralleling regulatory concerns with the iOS app store). As a tech giant Meta can moreover afford to undercut competitors indefinitely on both hardware and software, excluding any meaningful competition.

While Australian regulators likely will have little ability to stop acquisitions (as these occur outside our jurisdiction), we recommend that the Senate consider other protective measures, such as regulating the extent to which infrastructure/platform providers are permitted to operate businesses that profit primarily from content.

Foreign Tech

Question 3: How should Australia and other countries approach regulation of cryptocurrency, including the CBDCs of other countries?

It is critical to note the distinction between cryptocurrencies and the broader category of digital currencies (central-bank digital currencies being a subset of the latter). While cryptocurrencies are understood as being part of a blockchain (a particular form of distributed record keeping system), digital currencies and other digital assets can be supported by databases of any sort.[22]

Cryptocurrency Investments

We turn first to the question of cryptocurrency regulation, recommending that investments in complex cryptocurrency products (such as *Initial Coin Offerings* and *Decentralised Autonomous Organisations*) be restricted to sophisticated investors *except* where they can meet similar requirements as those for securities.

Cryptocurrencies and other Blockchain-based projects have a substantial tie to scams, fraud, and direct consumer harms. Researcher Molly White has found that over $11 billion of losses globally are attributable to the "hacks scams and fraud since...2021". For mum-and-pop investors, even the best of projects have an usually high rate of "going to zero"[23]. One potential cause is the disconnect between marketing documents (*whitepapers*) and the actual code that runs blockchain projects. In one of our studies "Coin-Operated Capitalism"[24] we found that of the top-fifty blockchain projects failed to add code to their projects to make-good on their promise. As of writing, the vast majority of investors in the fifty projects are left with nothing to show.

The strongest argument against regulation is the suggestion that sophisticated investor rules magnify social inequities by denying small investors access to the projects that offer the largest potential upside. However, as found in our research, there is a lack of market discipline and a severe information asymmetry–this means that even were small-time investors to retain access to blockchain projects, the overwhelming likelihood is that it will end in ruin over riches.

---

[22] Indeed one digital currency issued in 2021 was notable for being issued based on a simple spreadsheet document: 'Roy's NFT Emporium on Web 3.0 by roycoding' *CSVCHAIN.com* (Website) <https://csvchain.com/>.
[23] 'How crypto goes to zero' *The Economist* (23 November 2022).
[24] Shaanan Cohney, David Hoffman, Jeremy Sklaroff and David Wishnick, 'Coin Operated Capitalism' (2019) 119(3) *Columbia Law Review* 591.

As a result, our research suggests that the wisest path forward is to restrict complex investments in blockchain projects to sophisticated investors, where such investments have not met a bar similar[25] to those faced by ordinary issuers of securities.

To meet the remedial need for consumers affected by fraud, there is significant virtue in ensuring that Australian private law accommodates the broader category of rivalrous digital assets. Work establishing such a regime has been undertaken in the UK, drawing extensively upon our research,[26] and will shortly come to conclusion.

Big Tech

Question 1: What impact does the market power of big tech companies have on the economy, society and small businesses?

The impact of Big Tech's market power is well documented, and there exists a vast body of research and commentary on the topic expounding both their positive and negative impacts.

We suggest that further inquiry into big tech be narrowed to specific questions of interest. Here we address two areas of concern: economic impact, and disinformation.

Economic Benefits and Harms

The market power of big tech has both positive and negative impacts on the economy. We outline several of these below, as well as proposals for reform, to provide direction for further inquiry. We notably do not take a stance as to the extent danger posed by the harms, nor their weighting against the benefits.

Benefits

- Convenience, affordability, efficiency: The ACCC recently acknowledged that both Australian consumers and business benefit from the convenience and efficiency of digital platform services, for such things as shopping, searching, and communicating.[27] This is made possible by the fact that the vast majority of the population uses the same platform for these activities, meaning the platform can effectively aggregate information

[25] We note that narrowly tailored rules for crypto-securities may differ in specifics to those for ordinary securities. We merely assert that there should be a similar level of disclosure and legal stability.
[26] In the context of Law Commission Consultation Paper 256, see e.g. Tatiana Cutts, "Possessable Digital Assets", LSE Policy Briefing Series #47 2021, and Tatiana Cutts, "Assets Represented By Computer Code: Response To "Digital Assets: Law Commission Consultation Paper 256" (LSE Law Policy Briefing Paper #50).
[27] ACCC, 'Digital Platform Services Inquiry – September 2022 Interim Report' (Report, 11 November 2022) 29 (s 1.3).

for users to access.[28] For instance, the ACCC has found that Google holds 94% of the market for search engine services.[29]

- Accessible display advertising: Business in particular benefit from the ability to reach and engage with a larger audience, as well as make use of resources for the development of applications and other tools.[30] This is similarly facilitated by the large user bases of digital platform services like Google search and Facebook.[31]

Harms

Alongside these benefits, the significant market power enjoyed by digital platforms can[32] *and does*[33] have negative impacts on the economy. These include (of which several are noted in the issued paper): [34]

- Killer acquisitions: Killer acquisitions refer to the practice of acquiring competitors to shut down or take control of projects that threaten a platform's dominance or market share—a well-known phenomenon on the pharmaceutical industry.[35] The most well-known instance of this conduct in the digital platforms context is Facebook's acquisition of Instagram in 2012, which Facebook considered a 'threat'.[36] This has a deleterious effect on competition and obviates the potential benefits of innovative new services.
- Predatory pricing: Amazon has a well-documented practice of forcing competitors out of business by undercutting prices of similar goods on their marketplace platform, followed by subsequent price rises once the competitor is eliminated. [37] This results in the usual negative impacts from reduced competition, such as reduced choice, higher prices, and less variety among similar goods, resulting in undesirable outcomes for consumers.

---

[28] For an exposition of aggregators in the context of digital platforms, see Ben Thompson, 'Defining Aggregators' *Stratechery* <https://stratechery.com/2017/defining-aggregators/>. Also ACCC (n 26) s 1.3.
[29] ACCC, 'Benefits from more competition in internet search' (Web Page, 28 October 2021).
[30] Ibid
[31] ACCC 'Digital Advertising Services Inquiry – Final Report', 4.1.1 (pp 88 – 89).
[32] See Mansell and Steinmeuller, 'Advanced Introduction to Platform Economics' ch 3, 43 'Whether market dominance will be contested is an empirical question'.
33 Compare above comments with Leshui He, Imke Reimers and Benjamin Shiller, 'Does Amazon Exercise its Market Power? Evidence from Toys"R"Us' 64(4) *Journal of Law and Economics* 635, 679 – 680, finding that toy prices increase on Amazon after Toys"R"Us bankruptcy; Lina Khan, 'Amazon's Antitrust Paradox' 126(3) *Yale Law Journal* 564, 768-9 on Amazon's 'killer acquisition' of Quidzi, and generally about flawed assumptions of entry and exit barriers.
34 Senate Economics References Committee, 'Inquiry into international digital platforms operated by Big Tech companies – issues paper' (Senate Inquiry Consultation Paper, 2022) 5-10.
[35] C.f. Florian Ederer, 'Does Big Tech Gobble Up Competitors?' *Yale Insights* (4 August 2021) <https://insights.som.yale.edu/insights/does-big-tech-gobble-up-competitors>.
[36] C.f. Rob Price, 'Zuckerberg viewed Instagram as a threat that could hurt Facebook's business before buying it, internal emails show' *Business Insider* (30 July 2020).
[37] C.f. He et al (n 32); Khan (n 32).

- Suppression of innovation:[38] In addition to the effect of predatory pricing and killer acquisitions, platforms are known to engage in other conduct that suppresses innovation. For instance, Amazon is known to use sellers' data to create their own cheaper house-brand alternatives, and[39] Facebook has been accused of copying a competitor platform's features after the competitor declined a merger. [40] Such conduct imperils economic incentives to innovate by threatening the custom a potential competitor might receive.
- 'Digital rentiership':[41] Digital rentiership refers to platforms extracting discommensurate rewards for their services relative to the benefit they provide to society. Examples of rentiership include Apple's 'walled garden'[42] ecosystem which 'locks' users in by making interoperability between different systems (e.g. Android) difficult, thus allowing Apple to charge higher prices than they would if they had to compete on quality of product and service alone.
- Self-preferencing:[43] Self preferencing is where digital platforms treat their own services more favourably on the platform than their competitors. Key examples of this include pre-installed web browsers such as Safari on iOS, or Google demoting rival shopping aggregator search results in favour of its own service.[44]
- Reliance resulting in imbalance of bargaining power: The prevalence of social media marketing[45] illustrates the degree of interdependence between small business and Big Tech; with small business needing to put their product 'out there' on these platforms, while big tech gains advertising revenue and stands to gain from the wealth of user-generated data in its own interests.[46] Further economic concern stems from SME's

[38] See OECD, 'Start-ups, killer acquisitions and merger control' (Web Page) <https://www.oecd.org/competition/start-ups-killer-acquisitions-and-merger-control.htm> In the Digital Platforms context see Khan (n 32), but see Renaud Foucart, 'Tech firms face more regulation after moves to stop 'killer acquisitions' – but innovation could also be under threat' *The Conversation* (25 July 2022) <https://theconversation.com/tech-firms-face-more-regulation-after-moves-to-stop-killer-acquisitions-but-innovation-could-also-be-under-threat-187278>.

[39] Aditya Kalra and Steve Stecklow, 'The Imitation Game – A Reuters Special Report' *Reuters* (31 October 2021) https://www.reuters.com/investigates/special-report/amazon-india-rigging/

[40] Billy Gallagher, 'Copycat: How Facebook Tried to Squash Snapchat' *Wired* (16 February 2018) <https://www.wired.com/story/copycat-how-facebook-tried-to-squash-snapchat/>; Nix (n 19) and text to n 19.

[41] Kean Birch and DT Cochrane, 'Big Tech: Four Emerging Forms of Digital Rentiership' (2022) 31(1) *Science as Culture* 44.

[42] See e.g., Jon Swartz, 'Apple has spent decades building its walled garden. It may be starting to crack' *MarketWatch* (7 May 2022) <https://www.marketwatch.com/story/apple-has-spent-decades-building-its-walled-garden-it-may-be-starting-to-crack-11651762698>; text to n 20.

43 See e.g. Christophe Samuel Hutchinson and Diana Treščáková, 'Tackling gatekeepers' self-preferencing practices' (2022) 18 *European Competition Journal* 567.

[44] Brody Mullins, Rolfe Winkler and Brent Kendall, 'Inside the U.S. Antitrust Probe of Google' *The Wall Street Journal* (New York, 19 March 2015).

[45] Helena Alves, Cristina Fernandes and Mario Raposo, 'Social Media Marketing: A Literature Review and Implications' (2016) 33(12) *Psychology & Marketing* 1029.

[46] Senate Economics References Committee (n 33) 14.

reliance on big tech for services needed for day-to-day operations.[47] Such reliance allows platforms to impose exploitative agreements on sellers for instance.[48]

Proposals for reform

Proposals for reform to address these harms, relevant to the Australian context, have been detailed extensively by the ACCC in their various reports from the Digital Platform Services Inquiry.[49] We support the following reforms in particular:

- Prohibition on unfair trading: We support the introduction of a prohibition on unfair trading,[50] to better address systematic undesirable business practices and models than the current suite of consumer and competition laws allow. We refer you to our recent submission to the Department of Treasury for a more detailed explanation of our position.[51]
- Competition law reform: We are broadly supportive of calls to reform Australia's merger laws,[52] and to strengthen competition law more generally[53] to address the above-mentioned anticompetitive behaviour of digital platforms.
- Other reforms: We further note that not all harms arising from the market power of digital platforms are able to be addressed by market- and consumer-based regulation. For instance, while agreements permitting expansive collection of personal data could (and indeed should) be scrutinised through the Unfair Contract Terms Law,[54] reforms to Privacy Law[55] play a significant role in addressing harms arising from such agreements.

Information Harms

A key social concern related to Big Tech's market power is the proliferation of disinformation which allows Big Tech through their platforms to influence an *epistemic*

---

[47] This includes digital marketing services, IT infrastructure such as email servers and website hosting, and importantly payment processing.
[48] See e.g., Annie Palmer and Jordan Novet, 'Amazon bullies partners and vendors, says antitrust subcommittee' *CNBC* (6 October 2020).
[49] 'Digital Platform Services Inquiry 2020 - 25' *ACCC* (Web Page) <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25>.
[50] See e.g. 'ACCC calls for new competition and consumer laws for digital platforms' *ACCC* (Media Release, 11 November 2022) < https://www.accc.gov.au/media-release/accc-calls-for-new-competition-and-consumer-laws-for-digital-platforms>.
[51] Shaanan Cohney, Liam Harding and Suellette Dreyfus (CAIDE), Submission to Department of Treasury, *Digital Platforms – Consultation on Regulatory Reform* (14 February 2023) 15, accessible at <https://www.unimelb.edu.au/__data/assets/pdf_file/0008/4504634/Strengthing-Australian-Consumer-Protection-in-the-era-of-Digital-Platforms-14-Feb-23.pdf>.
[52] See generally Rod Sims, 'Don't bother pleading with banks to be nice. They're too busy synchronised swimming' *The Age* (17 February 2023).
[53] 'ACCC calls for new competition and consumer laws for digital platforms' *ACCC* (Web Page, 11 November 2022) <https://www.accc.gov.au/media-release/accc-calls-for-new-competition-and-consumer-laws-for-digital-platforms>.
[54] ACL (n 13) Ch. 2, pt. 2-3, ss 23, 24.
[55] Attorney General's Department, 'Privacy Act Review' (Report, 2022).

environment (simply, the environment from which one gets credible information). This can have several negative impacts on such things as democracy, community safety and social cohesion.

Evidence and Harms

Several recent inquiries and experiences illustrate Big Tech's influence on Australians' access to information:

- During a brief period in 2021 when Facebook temporarily banned the publishing of news by Australians on its platform,[56] reputable news sources and smaller community organisations found themselves 'unpublished' and their posts deleted, while puzzlingly, conspiracy theories were left unaffected by the ban.[57] Facebook did so as a response to "legislation pressing digital giants to compensate publishers".[58] The ban was quickly reversed weeks after.
- Statistics from the UK regulator OfCom identified that "29% of teens used Meta Platform Inc's Instagram to follow the news while TikTok and Alphabet's YouTube were also used by 28% of teenagers for news".[59] This illustrates the ability of such tech giants to influence the overall landscape of news and information 'consumption habits' of its users, not always for the better.
- Existing research has pointed out various issues with the very nature of social media-as-a-news-source: propagation of misinformation online, limitations of automated fact-checking and content moderation, and the risk of radicalisation due to recommendation algorithms, amongst others[60].

---

[56] Samantha Dick and Cait Kell, 'Australians urged to break up with Facebook over news blockade' *The New Daily* (19 February 2021) <https://thenewdaily.com.au/news/national/2021/02/19/facebook-australia-news-break-up/>.
[57] Damien Cave, 'Facebook's New Look in Australia: News and Hospitals Out, Aliens Still In' *The New York Times* (18 February 2021) <https://www.nytimes.com/2021/02/18/business/media/facebook-australia-news.html>.
[58] Livia Albeck-Ripka, 'Facebook Agrees to Pay for Murdoch's Australia News Content' *The New York Times* (16 March 2021) <https://www.nytimes.com/2021/03/16/business/media/news-corp-facebook-news.html>.
[59] Farouq Suleiman and Jonathan Oatis (ed), 'UK teens shun traditional news for TikTok, Instagram – Regulator' *Reuters* (21 July 2022) <https://www.reuters.com/business/media-telecom/uk-teens-shun-traditional-news-tiktok-instagram-regulator-2022-07-20/> as cited in Marc Cheong, 'Social Media Harms as a Trilemma: Asymmetry, Algorithms, and Audacious Design Choices' (Conference Paper, IEEE International Symposium on Technology and Society, 10 – 12 November 2022).
[60] Michel Croce and Tommaso Piazza, 'Consuming Fake News: Can We Do Any Better?' (2021) *Social Epistemology* <https://www.tandfonline.com/doi/full/10.1080/02691728.2021.1949643>; Deepa Seetharaman, Jeff Horowitz and Justic Scheck, 'Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts.' *The Wall Street Journal* (17 October 2019) <https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184>; Mark Alfano, Amir Ebrahimi Fard, J Adam Carter, Peter Clutton and Colin Klein, 'Technologically scaffolded atypical cognition: the case of YouTube's recommender system' (2021) 199 *Synthese* 835.

- The propagation of COVID-19 misinformation[61] online during the pandemic serves as a particularly stark and consequential example of dis- and misinformation on digital platforms.

Reform proposals

In considering whether and what regulatory reform is necessary to combat dis- and mis-information on digital platforms, data must be made available to researchers and policy makers in order to better understand the nature and scope of the issue. To this end, we are supportive of several reforms:

- Platform data for public interest research: Unfortunately, the lack access to platform data remains a significant roadblock in analysing the phenomena of mis- and disinformation. We refer you to our submission to the Department of Treasury for further exposition of this issue.[62] We are therefore supportive of mandatory reporting requirements for digital platforms, with data to be reposed with a regulator such as the ACCC or the Australian Communications and Media Authority (ACMA). Exact reporting requirements should be developed in consultation with research organisations. We further note that voluntary disclosure regimes have not achieved stated outcomes in foreign jurisdictions.[63]
- Protection of public interest researchers: Researchers investigating harms of digital platforms have in the past been subject to reprisals and hindrances by the platforms themselves. We again refer you to our submission to the Department of Treasury for further comment on this matter.[64]
- Enhanced data analysis capacity for regulators: For similar reasons detailed earlier in this submission, [65] we recommend that the ACCC and ACMA be equipped with enhanced technical research and data science capabilities–through recruitment of technical personnel. In conjunction with data available from mandatory reporting, this will allow the relevant regulator to undertake their own independent investigations, rather than relying solely on platforms themselves to disclose efforts to combat dis- and misinformation.

---

[61] Michael A Gisondi, Rachel Barber, Jeremy Samuel Faust, Ali Raja, Matthew C Strehlow, Lauren M Westafer and Michael Gottlieb, 'A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation' (2022) 24(2) *Journal of Medical Internet Research* <https://doi.org/10.2196/35552>.
[62] Cohney, Harding and Dreyfus (n 50) 18 – 20.
[63] See e.g., ACMA, 'Misinformation and News Quality on Digital Platforms in Australia – A position paper to guide code development' (Position Paper, June 2020) 15 – 16.
[64] Cohney, Harding and Dreyfus (n 5), 18 – 19.
[65] See text to note 2; Centre for Artificial Intelligence and Digital Ethics, Submission to Department of Treasury, *Digital Platforms Inquiry – Consultation on Regulatory Reform* (14 February 2023) 17-18, available at: <https://www.unimelb.edu.au/__data/assets/pdf_file/0008/4504634/Strengthing-Australian-Consumer-Protection-in-the-era-of-Digital-Platforms-14-Feb-23.pdf>.

Respectfully submitted with contributions from:

Gabby Bush

Dr. Marc Cheong

Dr. Shaanan Cohney*

A/Prof. Tatiana Cutts

Dr. Suelette Dreyfus

Liam Harding*

A/Prof. Toby Murray

Dr. Sarita Rosenstock

* Indicates principal responsibility for drafting and redacting the submission