Where to for protected digital disclosures in Australia?

Reset.Tech Australia and
Human Rights Law Centre
December 2024
Policy briefing

Version 1.0

Human Rights Law Centre

Electronic Frontiers AUSTRALIA

Reset·Tech AUSTRALIA

Contents

This document is a read-out from a closed-door discussion on public accountability and tech whistleblowing. It is presented as a summary of early policy thinking, representing perspectives from tech and accountability advocacy, media, and law. Accordingly, this document is early-stage rather than exhaustive, and will continue to be iterated on.

About the lead authors

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

The Human Rights Law Centre uses strategic legal action, policy solutions and advocacy to support people and communities to eliminate inequality and injustice and build a fairer, more compassionate Australia. In 2023, we launched the Whistleblower Project, Australia's first dedicated legal service to protect and empower whistleblowers who want to speak up about wrongdoing. We provide legal advice and representation to whistleblowers, as well as continuing our longstanding tradition of advocating for stronger legal protections and an end to the prosecution of whistleblowers. We are also a member of the Whistleblowing International Network. Digital products and technological industries bring innovation and promise, yet also carry with them a range of risks and harms – many of them with a strong nexus to human rights threats. Our understanding of extant and emerging harms continues to be reliant on whistleblower disclosures.

Introduction

Australia is a lively site for digital accountability debates, but these debates suffer from incomplete evidence on technology risks and harms. In addition, Australia has been labelled one of the most secretive democracies in the world,[1] due to extensive government surveillance powers and a generally perilous environment for whistleblowers. Public trust in government is backsliding, and transparency – whether into government or into tech companies – is collapsing. A healthy and increasingly digital democracy cannot survive without safe and reliable avenues for public scrutiny and accountability.

Australia, like many democracies, faces a dual situation of low public trust towards Big Tech and equally towards government. Even with well-designed platform accountability and transparency laws, the success of these measures rests on the public's confidence in governments to deliver them. Consider, for instance, the Australian Government's two major legislative moves on tech accountability – the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* and the *Online Safety Amendment (Social Media Minimum Age) Bill 2024*. The former ultimately failed to gain support in the Senate, in part due to a debate that was deeply affected by low trust in government and associated regulators. The latter 'prevailed' through a condensed parliamentary process with limited opportunity for public scrutiny. It has additionally unlocked a suite of new issues around digital privacy and government surveillance. Learning from the failed misinformation bill especially, public trust issues cannot simply be counter-messaged; they must be addressed through government measures that meaningfully create accountability and transparency to the public.

Whistleblowers serve an essential public function. By exposing wrongdoing, whether in government or in companies, whistleblowers contribute to democratic accountability and good government. But too often, whistleblowers suffer when they speak up – which has a chilling effect on prospective whistleblowers. Research shows that as many as 8 in 10 whistleblowers experience some form of workplace retaliation; recent high-profile cases have seen whistleblowers face lawsuits and even prosecution. This landscape raises critical questions about how to foster whistleblowing in the tech context.

This policy briefing summarises a discussion held in November 2024 with a group that brought expertise across public interest journalism, digital platform accountability, whistleblower protection, human rights and digital rights, and the tech sector itself. Provocateurs spoke to three themes, which were:

1. What are the current mechanisms for digital protected disclosures in Australia?
2. How are tech whistleblower disclosures reaching journalists?
3. How are courts using whistleblower evidence in litigation?

The recommendations provide a template for timely and targeted reforms which will be of interest to state and federal decision-makers.

[1] Most prominently by Damien Cave, 'Australia May Well Be the World's Most Secretive Democracy', *New York Times* (online, 5 June 2019) <https://www.nytimes.com/2019/06/05/world/australia/journalist-raids.html>.

1. What are the current mechanisms for digital protected disclosures in Australia?

Whistleblowing is a significant component of the tech accountability movement overseas, but is yet to emerge to the same extent in Australia. In the last few years there has been a wave of tech accountability in the United States, United Kingdom and Europe, matched by a wave of support to civil society organisations and nonprofits for tech accountability in general. But Australia has not seen a similar wave in tech whistleblowing, whether as a working concept or as a source of evidence driving corporate accountability.

Whether in the digital realm or not, Australian whistleblowers are protected under law but those laws are not working in practice. There are some practical challenges that whistleblowers in Australia face, and potential whistleblowers need guidance and support through this process. Human Rights Law Centre and Reset Tech Australia, along with numerous expert partners, are releasing a guide on digital whistleblowing. Where many of the guides overseas focus on a narrower definition of tech whistleblowing that is Silicon Valley-centric, this guide adopts a broader definition that examines a range of digital sectors, including downstream providers.

There are existing pathways for making a protected disclosure in Australia about sector-specific digital and technology issues. The *Corporations Act* (s 1317AA) provides for disclosures on misconduct or an improper state of affairs in relation to a company. However, currently only ASIC[2] and APRA[3] are prescribed by the Act to receive these disclosures. s 1317AA 1(b)(iii) anticipates other Commonwealth authorities to be recipients of protected disclosures, but further recipients have not yet been provided for by regulation.[4]

Australia has four key regulators covering digital issues (eSafety Commissioner, Office of the Information Commissioner, Australian Communications and Media Authority, Australian Competition and Consumer Commission), who share information and collaborate via an initiative called DP-REG.[5] Note, DP-REG is "not a decision-making body, and has no bearing on members' existing regulator powers, legislative functions or responsibilities".[6]

Realistically speaking, Australia won't have a Facebook product manager blowing the whistle tomorrow; the idea is to nurture a role for potential digital whistleblowers. Australia continues to be a lively site for tech policy debate but this debate has suffered from an absence of insider information on harms and corporate conduct. Policymaking has been hindered as a result, as there are such limited ways to adduce evidence on what's happening under the hood with digital products and services.

To address the worst excesses of harmful digital companies (and governments deploying harmful digital tools) Australia needs people to be able to step up and disclose wrongdoing that exists, and have a legal framework to do so. The European Union has gone as far as launching an online whistleblowing portal for concerns relevant to the *Digital Services Act* and the *Digital Markets Act*. In contrast, none of the relevant Australian regulators have the ability to receive protected disclosures. Regulators that can receive protected disclosures do not tend to have a particular interest in digital concerns.

---

[2] Australian Securities and Investments Commission, 'Make a report of misconduct to ASIC' (Web Page, 30 June 2023) <https://asic.gov.au/about-asic/contact-us/reporting-misconduct-to-asic/make-a-report-of-misconduct-to-asic/>.
[3] Australian Prudential Regulation Authority, 'Make a complaint about an APRA-regulated entity' (Web Page, 2024) <https://www.apra.gov.au/make-a-complaint-about-an-apra-regulated-entity>.
[4] *Corporations Act 2001* (Cth) s 1317AA 1(b)(iii) provides, 'a Commonwealth authority prescribed for the purposes of this subparagraph in relation to the regulated entity'.
[5] See Australian Government, *Digital Platform Regulators Forum* (Web Page, 2024) <https://dp-reg.gov.au/>.
[6] See DP-REG, 'Terms of Reference'(7 July 2022) <https://www.oaic.gov.au/__data/assets/pdf_file/0019/16732/DP-REG-Terms-of-Reference.pdf>.

2. How are tech whistleblower disclosures reaching journalists?

Practically speaking, journalists find it challenging to support people to blow the whistle in Australia. There are a range of issues with the current whistleblower protection framework, and there's also interconnected issues that affect journalists' ability to protect whistleblowers' identities. There are a range of mechanisms that work against journalists' abilities to ensure anonymity of their sources, including the TOLA Act and anti-encryption laws, metadata retention laws, a general lack of judicial oversight on granting data access, and the conditions that gave rise to the now-infamous AFP raids on the ABC and Newscorp. These contribute to a general sense of nervousness around coming forward in Australia on public interest concerns. Improving protections for journalists gets a lot of attention, but we also need to protect the whistleblowers too. Their interactions with journalists are a small part of the whistleblowing process, and they need protections throughout the journey of making disclosures.

In focus - AN0M and digital interceptions

The facts of AN0M have opened up questions around admissibility of evidence, particularly what is considered to be an interception for the purposes of *s 7(1) of the Telecommunications (Interception and Access) Act 1979*. AN0M was a scheme run between the Australian Federal Police and the United States' Federal Bureau of Investigations. The objective was to create a honeypot-style encrypted application that would be used by underworld figures in their communications and accessed by authorities to make arrests. Under the belief the correspondence on the application was secure, underworld figures transmitted messages between each other that provided vivid insights to authorities into various criminal activities, including money laundering and drug trafficking.[7]

The content of these messages was used by police to arrest dozens of alleged offenders, and was relied upon as key evidence. Those charged with the offences argued that the authorities' use of the messages was not legal, as the 'interception' had been made without an interception warrant. The accused argued the evidence was inadmissible. A question of law was asked of the South Australian Court of Appeal, primarily on issues of admissibility.[8]

The Court of Appeal agreed with the Director of Public Prosecutions' argument that no interception had occurred. This argument rested on technical evidence that the copy of the original message sent to the server where authorities had access was made *within the AN0M device itself* and *prior to the message's transmission*. In November 2024, special leave was granted to the High Court for an appeal. Later in the month, Parliament passed the *Surveillance Legislation (Confirmation of Application) Act 2024*, which clarified that the relevant information 'was not intercepted while passing over a telecommunications system and was lawfully obtained under those warrants, consistent with the Parliament's intention'.

Evidently, the Government is making efforts to ensure this particular class of surveillance survives review in the courts, and has a path to continue in practice. This is happening by arguing that the surveillance activity is factually carved out from being an 'interception' as defined in the Act.

[7] South Australian Office of the Director of Public Prosecutions, 'Questions of Law Reserved (1 and 2 of 2023)' (online, 27 June 2024) <https://www.dpp.sa.gov.au/prosecuting-crimes/cases-of-interest/questions-of-law-reserved-1-and-2-of-20232024sasca-82-27-june-2024>

[8] Ibid.

In focus - Secrecy Offences – Review of Part 5.6 of the *Criminal Code Act 1995*

Earlier in 2024, the Independent National Security Legislation Monitor released a series of recommendations relating to Australia's secrecy offences. A number of these focus on the nexus between 'non-officials' (such as journalists) and secrecy offences. The report set out four relevant secrecy principles for non-officials:

1. Secrecy offences should relate squarely to the communication of information,
2. The focus of secrecy offences should be on the actual harms,
3. The application of secrecy offences should only be to serious harms, and
4. Offences against non-officials should be narrower than offences for officials.[9]

In November 2024, the Australian Government accepted the report's recommendation to repeal a provision in the *Criminal Code* that makes it an offence for journalists to receive certain sensitive or classified information.[10] This is welcome progress, signalling that future reforms will seek to address the excesses of secrecy laws and their purported chilling effect on public interest journalism and oversight of national security and law enforcement.

Australia desperately needs whistleblowers to come forward on digital issues. Digital platforms in particular are so opaque, and transparency into their systems is totally collapsing. It's getting harder and harder for journalists to see what is going on under the hood. Whistleblowers are certainly widening in their importance as a source of public transparency and corporate accountability.

The chilling effect is real, both in the sense of whistleblower disclosures and access to information on corporate tech conduct. Australian whistleblowers continue to be sued and put in jail. And on the tech transparency front, despite some good progress on independent data access to digital platforms, this ultimately didn't stick, and we're back to square one of a diminishing transparency environment. Whistleblowers need safer ways to come forward, and to do so in a fashion that matches the fast pace and high stakes of online dangers and harms. Beyond whistleblower frameworks, there are some severe chilling effects in defamation law, freedom of information frameworks,[11] and a general lack of good information from government departments.

[9] See generally, Australian Government Independent National Security Legislation Monitor (INSLM), *Secrecy Offences – Review of Part 5.6 of the Criminal Code Act 1995* (2024) <https://www.inslm.gov.au/publications/secrecy-offences-review-part-56-criminal-code-act-1995>.

[10] Australian Government Independent National Security Legislation Monitor (INSLM), *INSLM welcomes government response to secrecy review* (Web Page, 27 November 2024) <https://www.inslm.gov.au/news-and-media/inslm-welcomes-government-response-secrecy-review>.

[11] See in particular, over-reliance on exemptions from disclosure, as well as the under-rescouring of responsible regulatory bodies such as the OAIC.

3. How are courts using whistleblower evidence in litigation?

In the US, platform accountability advocates feel structurally constrained by a relative absence of a regime providing legislated transparency measures, due to concerns with the First Amendment. As a result, those in the jurisdiction struggle to understand how Big Tech companies operate from the inside, and oftentimes whistleblower evidence is the best available to demonstrate how decisions are made internally, and to offer that evidence in court. This evidence is particularly helpful for adducing issues of corporate intent.

Whistleblower evidence is particularly useful for issues around how executive decision-makers did or did not make certain decisions, despite being aware about potential or actual harms and foreseeable dangers of their products or activities. Litigation and legislation are two sides of the same coin and so the whistleblower testimonies also play a role in activating lawmakers and the public in order to achieve greater accountability. It has been particularly explosive in terms of opening up the public conversation.

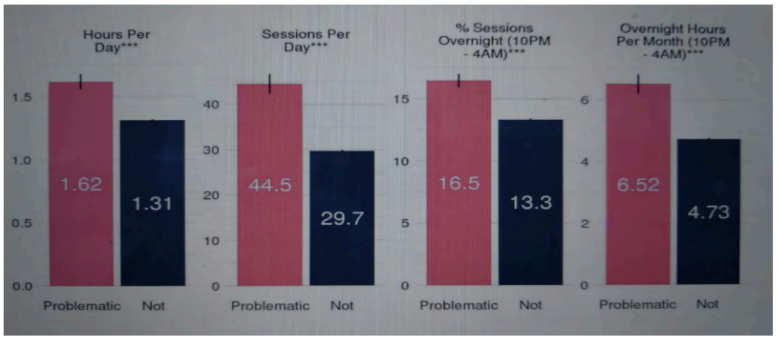
Whistleblower evidence features prominently in a range of litigation on foot against TikTok, Snap, Meta, and Google, brought by numerous stakeholder groups, including families impacted by harms to their children, hundreds of school districts, and state Attorneys General.[12] Inside these complaints are heavily redacted documents, including from whistleblowers, and for the Meta cases, many of these the Facebook Papers brought forward by Frances Haugen.[13]

In focus: Facebook Papers in the courts

An example from a complaint run by the Social Media Victims Law Center[14] in the US, which meticulously drew upon evidence from the Facebook Papers to validate the plaintiff's arguments, particularly around the company's knowledge of its dangers and potential harm to children.

14. Specifically, Meta leadership has vehemently denied that its products are harmful or addictive. Meta has gone to great lengths to assure the world that its social media products are safe. Even its Terms of Use (effective January 4, 2022) represent that Meta is "Fostering a positive, inclusive, and safe environment," and that Meta uses its "teams and systems … to combat abuse and violations of our Terms and policies, as well as harmful and deceptive behavior. We use all the information we have—including our information—to try to keep our platform secure." (Effective January 4, 2022). However, Meta's own internal research and "experiments" show the opposite. The Facebook Papers include years' worth of studies and reports, often referred to by Meta as "experiments," discussing the fact that Meta's social media products are addictive and harmful, and that use of those products can and does lead to serious mental health issues in a significant number of users, including things like anxiety, depression, eating disorders, and what Meta refers to as Suicide and Self Injury (or, SSI). The following are just a few examples.

[12] See for example Rebecca Kern, Josh Cisco, Alfred Ng 'Dozens of states sue Meta over addictive features harming kids' *Politico* (online, 24 October 2023) <https://www.politico.com/news/2023/10/24/states-sue-meta-addictive-features-kids-00123217>.
[13] See Tech Law Justice Project, *Big Tech Litigation Tracker* (2024) <https://techjusticelaw.org/2024/02/07/big-tech-litigation-tracker/>, and Kayleen Manwaring and Siddharth Narrain '41 US states are suing Meta for getting teens hooked on social media' (online, 13 November 2023) <https://www.unsw.edu.au/newsroom/news/2023/11/41-us-states-are-suing-meta-for-getting-teens-hooked-on-social-m>.
[14] Social Media Victims Law Center, *Spence Complaint – 6th June 2022* (2022) <https://socialmediavictims.org/wp-content/uploads/2022/06/Spence-Complaint-6_6_22.pdf>.



FBP 16/07, "Problematic Facebook use - when people feel like Facebook negatively affects their life" (July 31, 2018), at p. 15.

TL;DR

- *More time spent per session is associated with lower risk of problematic use.* Increasing a user's average time spent per session by 1s reduces a user's probability of problematic use by 0.03 to 0.1 percentage points.
- We should continue to *guard against disproportionate increases in short sessions* as we test product changes.

Note: for reference, the overall risk of problematic use was estimated to be about 3% as of April 2018.

FBP 16/00, "More time spent per session is associated with lower risk of problematic use" (August 19, 2019), at p. 2.

65. Recommendation-based feeds and product features also promote harmful content, particularly where, as in the case of Meta, the algorithm is being programmed to prioritize number of interactions and not quality of interactions,

- Recommendation systems are often prone to recommending bad content. As a simple example, every list I've ever seen of top content sorted by engagement rate (as opposed to overall engagement) has been heavily tilted towards problematic content. YouTube had a scandal around recommending conspiracy theories within the last six months, and the same phenomenon has been confirmed on Facebook.

SOCIAL MEDIA VICTIMS LAW CENTER PLLC
821 2ND AVENUE, SUITE 2100
SEATTLE, WA 98104
TELEPHONE: 206.741.4862

Discussion

The discussion centred around three themes.

The need for definitional breadth

- Many technology-related concerns in Australia transpire in the public sector use of tech. It's a tough topic, encouraging those in the Australian Government who have exposure to tech tools — especially in the national security and surveillance space — but it's necessary to consider. How do we encourage those who don't consider themselves tech workers, to nonetheless see themselves as advocates for accountable tech in government?

- The ongoing use of Clearview by Australian Government agencies is a good example, it's been publicly called out and made subject of an OAIC ruling, but some reports suggest it continues to be used. How can those in that space understand this is unacceptable and even unlawful, and what could encourage them to escalate their concerns internally? What products are out there? We need transparency about what tools are being used in Government for example, to provide leads and open up discussions about what the field is, to encourage whistleblowers.

- As noneof this technology is self-executing (yet), there are always people who know where dodgy technology is being deployed or bad decisions are made – the trick is encouraging those who know to be able to blow the whistle. Good tips can be hampered by a lack of documentary evidence. A constant fear of journalists is exposing their sources. The lack of protections for sources does undoubtedly prevent some stories moving forward.

Practical considerations

- **Availability of government information:** The New South Wales ombudsman report into all the algorithmic decision making tools being used in the state government earlier this year was an interesting but rare overview.[15] From a journalistic perspective, it offers a good process – start approaching people, start to encourage people to chat, and work from there. We need transparency from that angle to encourage leads, and also so that people within these companies, and within government, understand what kind of field they're playing in. There are also lists of the OAIC's commissioner-initiated investigations available from questions in Senate estimates.[16] We need to know where to look and who to ask and more transparency from government helps that – Senate estimates are a great avenue.

- **Reliability of information:** There is an ongoing challenge about getting good reliable sources of information. How do we find and encourage people with the 'right information' to come forward? Australia does not do well on accountability in general, and on whistleblowers specifically. No one who doesn't have accountability is jumping up and down to have more of it, but the public debate in Australia could be richer and more informed. The challenges around tech accountability arethe same as around tech policy in general – we are hampered by the issue of offshored global platforms, but this is a challenge to be solved rather than an excuse to block sensible reforms.

- **Keeping disclosures safe and protected:** Digital hygiene is under-discussed – this can end up as a blocker for prospective whistleblowers. If a source or whistleblower starts down this road without appropriate digital hygiene, it's very hard to undo. A lack of knowledge and

[15] NSW Ombudsman, *A map of automated decision-making in the NSW Public Sector: A special report to Parliament* (Report, 8 March 2024) <https://www.ombo.nsw.gov.au/reports/report-to-parliament/a-map-of-automated-decision-making-in-the-nsw-public-sector-a-special-report-to-parliament>.

[16] Office of the Australian Information Commissioner, *Senate estimates opening statement November 2024* (Online, 28 November 2024) <https://www.oaic.gov.au/news/media-centre/senate-estimates-opening-statement-november-2024>

awareness about how to disclose security and safety, or make initial first contacts, stymies what a person feels safe to disclose further down the track. There's room for best practice training and support for journalists working with whistleblowers. There are very few people who are dedicated tech journalists, but a lot of people have ended up reporting on tech, who may lack the confidence to report around this. We need an uplift for tech-adjacent people in the media and best practice protocols for journalists who work with sources.

Law reform opportunities

- **Formal pathways for protected digital disclosures:** We need to ensure that regulators can receive protected disclosures in a timely fashion, and that whistleblowers have a safe way to speak up. There's an opportunity to consider introducing reporting channels through the *Online Safety Act*, particularly if the statutory review emerges with recommendations to closely align to the *Digital Services Act*. But there's also other opportunities to consider this in the Privacy Act Tranche 2 amendments, and perhaps an overlooked route in the AI Act. At the moment the Government is pushing mandatory guardrails and principles around AI, but the sentiment is that this might have unintended consequences, and the more appropriate pathway might be law. This could be an opportunity to bake-in whistleblower protections on digital concerns specifically – although there is a need to ensure this is done consistently and harmoniously with existing whistleblower protection laws to avoid inconsistency and fragmentation. Best practice would be to ensure alignment between these digital laws and private sector protections in the *Corporations Act.* A low-hanging opportunity would simply be regulation to ensure digital regulators can receive disclosures.

- **Comprehensive whistleblower protections and a whistleblower protection authority:** A Private Members Bill was recently announced, to establish a federal whistleblower protection authority. Such a body would oversee public sector and private sector whistleblowers, and would encourage people to speak up, as well as identifying and addressing some of the regulatory gaps. It forms one part of the much-needed comprehensive reform geared to referring and assisting whistleblowers to take information to relevant parts of government and regulators. One of the challenges currently is that people don't know where to go, they don't know where they can go safely, lawfully, without risking jail, employment loss, and lawsuits. Note, there are other law reforms that should match this institutional reform. The protections in the US are lightyears ahead in terms of incentivising whistleblowers through financial support and the ability to take on cases, and hopefully Australia will start to catch up.

- **Leveraging extraterritorial applications**: More for implementation rather than reform, but a little-known component of the existing framework is around the extraterritorial application of Australian protections to non-resident whistleblowers.The law in extraterritorial application is complicated, but in theory where there is an affiliation with an Australian company or subsidiary, a whistleblower could draw on Australian protections. The exact protections will vary depending on the context, but this is part of the challenge and what is needed to open up a breadth of tech-related advocacy.

Recommendations

1. Law reform to ensure comprehensive whistleblower protections and the establishment of a Whistleblower Protection Authority
2. Reforms to key legislation to permit relevant digital regulators (ACCC, OAIC, eSafety, ACMA) to receive and act on protected disclosures
3. Educative measures for sources and prospective whistleblowers on digital hygiene
4. Comprehensive government reporting on use of technology by the public sector