Technology-Related Whistleblowing: **A Practical Guide**

Supporting whistleblowers in Australia to raise concerns about harmful digital systems and technology-related wrongdoing

Human Rights Law Centre

Reset·Tech AUSTRALIA

[Psst...]

DIGITAL RIGHTS WATCH

Lead Authors

Alice Dawkins, Executive Director, Reset Tech Australia
Kieran Pender, Associate Legal Director, Human Rights Law Centre

NOVEMBER 2024

Disclaimer

This Guide is intended to provide general information only and is not to be relied upon as legal advice. Readers should obtain their own information and up to date legal advice applicable to their individual circumstances. While every effort has been made to ensure the information is accurate at the time of publication of this document, we do not accept any responsibility for any loss or damage resulting from any error. This Guide is subject to applicable laws from time to time and should be read with your organisation's whistleblower policy (if they have one).

Acknowledgement of Country

We acknowledge the lands on which we work and live, including the lands of the Wurundjeri, Bunurong, Gadigal, Ngunnawal, Darug and Wadawurrung people. We pay our respect to Elders of those lands, both past and present. We recognise that this land always was and always will be Aboriginal and Torres Strait Islander land because sovereignty has never been ceded. We acknowledge the role of the colonial legal system in establishing, entrenching, and continuing the oppression and injustice experienced by First Nations peoples and that we have a responsibility to work in solidarity with Aboriginal and Torres Strait Islander people to undo this.

Acknowledgments

This guide has been developed in consultation with experts who have been painstakingly generous with their time and resources. These include Clayton Utz, for vital drafting assistance and legal expertise, and participants from a roundtable hosted by the Human Rights Law Centre and Reset Tech Australia in Canberra, in April 2024.

Human Rights Law Centre

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.

Reset Tech Australia

Reset Tech Australia is the Australian presence of Reset Tech. Reset Tech's mission is to guard against digital threats to our security, safety, and fundamental rights. We seek to "reset" the connection between media and democracy to restore the promise of technology that works for people and free expression. We work to hold the biggest tech companies accountable to the values of democratic societies by promoting new ideas to change laws, industry standards, and consumer attitudes.

Psst

Psst.org revolutionises the act of speaking out – making it a collective, safe, secure (and often world-changing) endeavor. By sharing stories collectively, strategically, and compellingly, the more information comes to light, the world pays attention, and we make holding companies accountable a lower-stakes prospect. Together, we change things for the better. So, if you are a concerned citizen, Psst....!

Digital Rights Watch

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

Foreword

Whistleblowing has become a critical source of public-interest evidence in the fight for safer technology products and to hold technology companies accountable.

Even as our economy shifts to a digital landscape, our public safety infrastructure remains heavily reliant on the public's ability to inspect products and the factories that produce them. Until corporate accountabilities expand to cover the full extent of Big Tech's behaviour and give the public the right to inspect digital systems, whistleblower disclosures are and will continue to be one of the few cracks of light we have into the cavernous domains of the powerful tech products and systems that shape our everyday lives.

I am first hand proof that information can transform what is possible when it comes to standing up for public safety. The documents I collected and provided to the US Congress and the SEC, now known as the Facebook Files, have been instrumental in sparking global conversations about the impact of social media on society and continue to play a role in making a case for legislative reform around the world for digital platform companies.

The Australian Government continues to signal big moves for tech accountability, but its project remains nascent. Australia is, in many respects, a testing centre for many of the world's incumbent tech giants and an incubator for the good, bad, and the unlawful.

Just in 2024, a wide variety of tech scandals came to light in Australia. Thousands of Australians' chest xrays were found to be used to train a private company's AI without their knowledge. A secretive, error-ridden, and "unscientific" algorithm was found determining the fate of Australia's immigration detainees. Personal photos of Australian children were found to be used to create powerful AI tools without the knowledge or consent of the children or their families. These powerful investigations by top reporters detail a taste of what's happening under the surface in data-powered, digital companies. There are almost certainly more.

New, digitally-directed legislation of various forms is making its way through lawmaking pipelines across domains of consumer protection, competition, privacy, and online safety. This is great news, as regulatory reform on digital platforms is overdue and essential. Yet it would be unfair and ineffectual to place the the complex challenges posed by the tech industry squarely on the shoulders of newly-empowered regulators. As Australia's eSafety Commissioner has said herself many times, we cannot purely regulate ourselves out of these problems.

We need multiple sources of accountability for tech companies, data firms, digital ecosystems – however they are defined. Yes, transparency reports into government regulators are one tool. But transparency is nothing without accountability. The lessons from the environmental movement and its big industrial incumbents reveal that we need many accountability levers. Encouraging accountability from the inside out in these companies is key, and nurturing a safe environment for whistleblowers to make protected disclosures is a critical step towards creating a more ethical and responsible digital landscape.

The depth, breadth, and pace of new digital risks are rolling out in real time. Timely disclosures will continue to be vitally necessary for getting a clearer picture of what risks and potential harm are arising from digital products and services. It is squarely in the best interests of both the public, and the companies themselves, for these risks to be known of and harms to be prevented. Organisations need not be hostile to whistleblowing – it is a practice that needs protection and encouragement. Put simply, protected tech whistleblowers make for better tech-enabled organisations.

This new guide for technology-related whistleblowing, co-authored by Human Rights Law Centre and Reset Tech Australia, provides a comprehensive overview of the pathways available to make protected disclosures on technology-related concerns in Australia. Knowing your options as a whistleblower is the first step towards what could be the most important decision in your life. Resources like Technology-Related Whistleblowing: A Practical Guide help make the disclosure journey a little less uncertain. The case studies in this guide may also surprise you – they may resonate in areas where you did not expect, encouraging the question – could I be a tech whistleblower?

Few people, if any at all, actively set out to be whistleblowers. It is a difficult and hazardous path, but sometimes it's the only path we have to serve the public interest, and even save lives. I commend this guide to you most highly.

Frances Haugen,
Tech whistleblower, author and public advocate

Image: Facebook Whistleblower Frances Haugen Opening Statement C-SPAN 2021

Navigation Menu

1. Introduction 8

1.1 Purpose of this Guide 8
1.2 Glossary 9

2. Overview 10

2.1 What is whistleblowing? 10
2.2 Why do we need whistleblowers to disclose harmful digital technologies? 11
2.3 Who is an eligible whistleblower in Australia 13

3. Blowing the whistle on digital technology concerns 14

3.1 What is a digital technology concern? 14
3.2 What types of disclosures are protected under Australian law? 15
3.3 When will digital technology concerns be covered by the whistleblower protections? 17

4. Before blowing the whistle 18

4.1 Things to think about before blowing the whistle 18
4.2 Who should I speak to first? 20
4.3 I have signed an NDA: does this affect my ability to make a disclosure? 20
4.4 Are there time limits? 21
4.5 What evidence do I need? 21
4.6 What if I have committed wrongdoing? 21
4.7 Can I be anonymous when making a disclosure? 22

5. Who can I make a disclosure to? 23

5.1 Who can I make a disclosure to under law? 23

6. Can I go to the media or a politician? 24

6.1 When should I go to the media or to a member of Parliament about my concern? 24
6.2 What is parliamentary privilege? 24
6.3 'Public interest disclosures' under the *Corporations Act* 25
6.4 Emergency disclosures under the *Corporations Act* 25

7. Protections for whistleblowers 27

7.1 How am I protected as a whistleblower? 27
7.2 What should I do if I suffer detriment? 28
7.3 Can I take the organisation to court if I suffer detriment? 29

8. Checklist of considerations when raising a digital technology concern 30

9. Case Studies 32

10. Summary of Australian Whistleblowing Laws 37

11. Personal Assessment Tool 52

12. Information Security 61

13. Endnotes 71

1. Introduction

1.1 Purpose of this Guide

Datafication, digitisation, and automation have encouraged the development of massive new companies and the rollout of digital products and services into most sectors and domains.

Digital technology companies – loosely referred to as constituting the 'tech sector' – have been the beneficiaries of at least two decades of preferential regulatory treatment, by governments encouraging innovation-driven economic upsides. This era of light-touch and industry self-regulation has encouraged 'blitzscaling'[1] (rapid growth and accumulation of new users) and what some experts have designated 'permissionless innovation'.[2] Products have increasingly been designed and deployed in a manner antithetical to notions of 'social license' or indeed, active and accountable consideration of the public interest.

This has led to a variety of risks and harms to the public, which are increasingly being exposed by whistleblowers. But not all harms start in Silicon Valley engineering suites. Companies are scaling around the world with risky products and harmful underlying datasets. Governments are seeking tech solutions that routinely create long tails of adverse consequences. Digital transformation has meant that more and more companies are trading in data or digital information and behaving like 'tech' companies.

This Guide has been prepared to help 'digital' or 'technology' whistleblowers speak up about any concerns they have in a safe and impactful manner. It provides guidance on whistleblowing, how to make a disclosure under Australian laws, considerations before blowing the whistle and the legal protections available.

The information contained in this Guide is general in nature and may not be suitable to your specific circumstances. If you would like further information, we encourage you to seek legal advice from the Human Rights Law Centre's Whistleblower Project legal service. The Project is Australia's first legal service dedicated to protecting and empowering whistleblowers to speak up about wrongdoing. The Project's legal service is free, and whistleblowers can contact it on a confidential basis.

1.2 Glossary

› **DISCLOSURE**

The act of making known information about wrongdoing, which a whistleblower has taken under a whistleblower law. Also referred to as a **Protected Disclosure.**

› **DISCLOSABLE MATTER**

An event, conduct, or series of actions by an individual or entity that can be made the subject of a whistleblower disclosure. It can also be considered **Wrongdoing**.

› **ELIGIBLE RECIPIENT**

An individual or entity that a disclosure can be made to, and be protected under a whistleblower law.

› **ELIGIBLE WHISTLEBLOWER**

Someone who is able to make a disclosure under whistleblower law and receive protections at law.

› **PID**

A "public interest disclosure". Under the PID legislation, this refers to any disclosure made under the legislation as a protected disclosure. Under some private sector laws, a public interest disclosure is made in certain circumstances where there is a risk to public health and safety, or the environment. In this Guide, PID refers to a public interest disclosure made under public sector PID legislation.

› **PID LEGISLATION**

Public interest disclosure legislation covering public officers and other individuals making disclosures about public sector bodies, which varies across states and territories, and in the federal jurisdiction.

› **PUBLIC OFFICER OR PUBLIC OFFICIAL**

An individual who is an employee of the Commonwealth, or a state or territory in Australia, or is otherwise appointed as a public officer. The definition of a public officer varies between jurisdictions, and you should check the relevant PID legislation to check the definition in relation to whistleblower protections.

› **VICTIMISATION**

When a whistleblower is treated badly or unfairly, or threatened with bad or unfair treatment, for having made a whistleblower disclosure. This is also sometimes referred to as **reprisal** or **detriment. Eligible whistleblowers** are protected from **Victimisation**.

› **WHISTLEBLOWER LAWS**

The collection of legislation across the public and private sector that provide protections for people who speak up about wrongdoing by making a disclosure.

2. Overview

2.1 What is whistleblowing?

Under Australian law, a whistleblower is typically an employee, contractor, volunteer or other worker who has access to information regarding wrongdoing, that is not otherwise known to the public, and alerts someone, either internally or externally, to that that information.

The disclosure of this information is whistleblowing. It is sometimes made to an internal whistleblowing mechanism, an external oversight body, or in some cases, straight to the public. Typically, whistleblowing involves disclosing incidents where law, misconduct or processes have been breached, which may include human rights abuses, fraud, corruption, maladministration, harassment, threats to health and safety or environmental wrongdoing. In these circumstances, an individual may be at risk of losing their job or being demoted. When an individual makes a disclosure via the correct pathway, they will be protected from retaliation, which means there may be legal remedies available if an employer causes them detriment.

In Australia, the law is complex and varies depending on whether the organisation who has committed the suspected wrongdoing is a federal or state/territory government agency or a private company. The threshold for whistleblowing and protections afforded to certain disclosures varies and expert legal advice is often necessary to determine correct procedures and the availability of protections. Whistleblowing has become a key form of drawing attention to wrongdoing, especially in business and government.

Without transparency there can be no accountability. Whistleblowers play a key role in exposing unlawful behaviour that would not otherwise be known, helping to ensure public accountability and safeguarding of the welfare of the environment and society.

Those who 'blow the whistle', as well as their colleagues and family, can face retaliation and suffer harm, such as damage to their reputation, career or financial position. Fear of retaliation and high profile cases have fostered a culture of silence and deterred people from speaking up about issues of concern. While people should be aware of the potential consequences of whistleblowing, this Guide will assist any person thinking of making a protected disclosure about digital and online concerns to do so safely and receive protections at law. These whistleblowers should seek appropriate legal support when coming forward.

2.2 Why do we need whistleblowers to disclose harmful digital technologies?

The growth of large technology companies has been tailed by a cascade of scandals, regular cycles of public concern, and routine calls for transparency and accountability. These risky systems and dangerous datasets are developed by organisations that run on, and by, human expertise. To keep the tech industry accountable to the standards of safety we hold as a society, it is important that individuals speak up when they see `any wrongdoing that could be a risk to the public; from the seemingly benign to the more serious kinds of weaponised technological harms.

The global tech whistleblowing movement has grown substantially in the last few years, with the development of highly impactful advocacy organisations and initiatives. These include, and are certainly not limited to, The Signals Network's 'Tech Whistleblowing Guides', and the related 'Tech Worker Handbook'. This Guide draws heavily on, and benefits greatly by, the work of these key projects. However, these works have been focused on Europe and the United States. The absence of public discussion about the potential for technology-related whistleblowing in Australia was among the sources of impetus for this Guide.

Some readers may be new to the concept of tech whistleblowing. Below are some key examples, which reflect both the geographic spread of whistleblowing, as well as the array of concerns – which span use and misuse of technical systems and data, to non-technical concerns of labour rights and safety. One takeaway from these examples, expanded upon in the section *'What is a digital technology concern?'* is to illuminate that relevant concerns can be both technical and non-technical in nature.

- **2015:** Erika Cheung, a lab assistant at biotech company Theranos, escalates concerns about the integrity of lab testing processes to federal authorities, and Wall Street Journal reporter John Carreyrou.
- **2018:** Christopher Wylie, an ex-employee of Cambridge Analytica, discloses to a Guardian/Observer investigation how digital personal information was used to build a profiling and targeting system to personalise political advertisements on social media.
- **2019:** Tang Mingfang exposes persistent labour rights violations at FoxConn, an Amazon supplier in China.
- **2021:** Frances Haugen shares over 20,000 internal Facebook documents, exposing the company's decision-making and culture around an array of risks and harms to the public. These become the source material for the Wall Street Journal's *Facebook Files* investigation and a number of complaints to the U.S. Securities and Exchange Commission.
- **2022:** Daniel Motaung, a former content moderator, speaks out on workplace safety concerns in a *Time* investigation into Sama, a Kenyan A.I. company responsible for commercial content moderation.
- **2022:** Mark MacGann, a former lobbyist for Uber, shares over 124,000 company files revealing tactics used to enter new markets and avoid regulation.

In the U.S., the 'tech whistleblower' ecosystem is defined, lively, and well-populated. By contrast, Australia is a 'net importer' of technology, meaning that the vast majority of risky digital technologies in use locally have been created elsewhere. As the Case Studies in this Guide illustrate, there are pathways for non-residents and non-citizens to make disclosures under Australian whistleblowing laws. This Guide also considers the multiple domains outside of an American-style 'tech whistleblower' framework that are relevant for urgent public interest whistleblower disclosures – data brokering companies, companies involved in significant data aggregation and data handling, and organisations involved in the procurement of risky digital technologies and systems, such as algorithms. Accordingly, this Guide should be read as a companion to, and deeply inspired by, 'tech whistleblower' literature.

At the time of this Guide's publication, Australia lacked a comprehensive and risk-based regulatory framework for digital platform companies. This means large digital platform companies are not under comprehensive requirements to assess risks to the public in their underlying systems. In this context of comparatively lighter-touch, relatively industry-driven self-regulation, it is especially important for whistleblowers to be able to safely disclose wrongdoing in tech companies.

Industry self-regulation need not be the only tool for tech accountability. Where sector-specific regulation exists, digital regulators simply cannot be the only line of defense. The depth, breadth, and pace of new risks is rolling out in real time. Tech accountability is a community effort - it takes concerned insiders, an engaged public *as well as* skilled public sector oversight to rein in the riskiness of the tech sector. Timely disclosures will continue to be vitally necessary for getting a clearer picture of what risks and potential harm are arising from novel digital products and services. It is squarely in the best interests of both the public, and the companies themselves, for these risks to be known of and harms to be prevented. Additionally, specific online safety or digital risk regulations need not be the only policy hook – there are rich areas for disclosures in existing legislation, such as misleading and deceptive conduct for the purposes of the *Australian Consumer Law*.

Another notable evolution to the sources of digitally-driven harms to the public is the rise of generative A.I. Relatively recent leaders in the A.I. space now more obviously join digital platform companies as potential harm producers. Significant risks to the public emerge along A.I's many 'supply chains', from data collection, to data labelling, to model training, to system deployment.[3] As one indicative example, a recent Human Rights Watch report identified how images of Australian children from personal, non-public collections had ended up in a dataset used to train popular A.I tools.[4] The unusual nature of the data's provenance raises questions about the data collection methods used, and is one example among many where whistleblower disclosures would shed timely light on practices in an under-regulated industry with obvious human rights impacts.

2.3 Who is an eligible whistleblower in Australia?

There are laws in Australia that set out protections to both 'public' and 'private' sector whistleblowers.

Part 10 of this Guide sets out who is an 'eligible whistleblower' within the public and private sectors in Australia. Other people who are not eligible whistleblowers can also raise concerns, however they may not have access to legal protections.

Public sector protections exist at the federal and state/territory level for whistleblowers who raise concerns about the public sector and matters of public interest.[5] Under these laws, an eligible whistleblower is a current or former 'public official', or, in some states and territories any person may make a disclosure under the public interest disclosure (**PID**) legislation.

Private sector protections exist under laws applying to corporations, taxation administration, registered organisations, aged care and the national disability insurance scheme. Under these regimes, an eligible whistleblower can include (depending on the law) an employee or contractor, volunteer, company director or officer, associate, trustee, custodian or investment manager of a superannuation entity or a spouse, relative or dependent.

Generally, people who fall into the following categories will not be covered by whistleblowing protections:

01. competitors to the organisation; and
02. customers and clients of the organisation.

3. Blowing the whistle on digital technology concerns

3.1 What is a digital technology concern?

There is no set definition for a 'digital technology concern', and the examples provided here are indicative and non-exhaustive.

Tech whistleblowing guides are typically constructed with massive production hubs like Silicon Valley in mind. Australia's landscape is a little different – for example routinely serving as a 'test market' for international companies eager to trial new product features or experiment with new market access tactics. It also, at the time of writing, has demonstrably weak regulations around privacy and data protection. One consequence of this is that the market is an attractive place for unethical and unscrupulous business practices in the domain of digital information and 'data' collecting and trading – practices that carry real-world harms to people in Australia.[6]

Some specific, hypothetical examples of the issues that could arise in an organisation are below. As the breadth of the examples demonstrate, a whistleblower into digital technology harms is *not only* a software engineer or product manager at a Silicon Valley tech company. They could be a public servant, a sector-specific startup, a company or government department involved in procurement, a digital marketing company involved in the 'data brokering' industry – the list of possibilities is extensive and the examples provided are far from exhaustive.

- A prison uses an algorithm to assess recidivism. No one is really sure how it works and there are suspicions that it is operating unfairly to produce adverse outcomes for inmates with particular characteristics.
- A local council is approached by an international tech platform. They enter into a partnership to encourage the development of innovative industries but in so doing ignore environmental and safety guidelines, as well as 'rushing through' decisions outside of the normal council procedure.
- A medical bookings platform collects and stores identifiable details of Australian users' visits to general practitioners. They ignore regulatory guidelines to store the data more securely and the company eventually suffers a massive data breach, exposing details of thousands of Australians to hackers.

- A real estate company procures an algorithm that draws upon inferencing techniques to 'rank' prospective tenants.
- An edtech startup knowingly harvests children's data (including their live location, browsing history, pages, addresses).
- A data broker facilitates the trading in sensitive information about people. Due to generally poor 'know your customer' standards across the industry, sensitive datasets on people in Australia are sold to scammers.

You do not have to be sure that the wrongdoing has in fact occurred in order to raise a digital technology-related whistleblower concern, but you should have some reasonable basis to form a belief or suspicion that wrongdoing has occurred.

A disclosure that later turns out to be incorrect can still be protected, however in most jurisdictions there is no protection for making a report that you know, or should know, is false, misleading or has no substance. Doing so may also expose you to disciplinary action by your employer.

3.2 What types of disclosures are protected under Australian law?

In the Australian private sector there are a number of different whistleblower laws which cover certain 'disclosable matters' that are eligible for legal protections. These types of disclosable matters are set out in more detail in Part 10.

Private Sector – *Corporations Act*

A 'disclosable matter' under the *Corporations Act* will arise where you have **reasonable grounds** to suspect that the information that forms your report concerns misconduct or an improper state of affairs or circumstances in relation to an organisation. There is no set definition of 'improper state of affairs' or 'misconduct', however, a disclosable matter may involve:

- fraud, negligence, default, breach of trust/duty or an improper state of affairs or circumstances relating to a company;
- an offence against a range of corporate and financial sector legislation specified under the *Corporations Act*;
- an offence against any law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more; or
- a danger to the public or the financial system.

The *Corporations Act* includes that in certain circumstances (see section 6.4) an emergency disclosure can be made in relation to information that the discloser has reasonable grounds to believe concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment.

You have 'reasonable grounds' if the information provides some support for your reported concern, for example, because it is based on something you have seen or heard.

CASE STUDY

Joe* and parliamentary privilege

The Human Rights Law Centre's Whistleblower Project assisted Joe* to blow the whistle on a fossil fuel company who covered up environmental harm.

We assisted Joe to provide evidence to a politician which showed the company had clearly caused significant environmental damage, and covered it up. Proof of the damage was subsequently tabled in Parliament, with politicians criticising the company for its actions.

This story was widely reported in the media, sparking public outrage at the company's lack of accountability for the environmental harm they had caused. Because of Joe's courage, Australians learned of harm to the environment. Joe triggered greater regulation and investigation of the company's response.

Joe did not suffer any retaliation and continues to work in his career.

Joe* is not the real name of this client.

Meaning of reasonable grounds

The idea of 'reasonable grounds' was considered in a recent case (*Quinlan v ERM Power Ltd* [2021] QSC 035) by the Supreme Court of Queensland. In that case, the judge said that:

- The information acted does not need to be based on a person's own observations; a person is entitled to form a belief based on what they have been told.
- A reasonable suspicion may be based on information which has been given to a person anonymously or which ultimately turns out to be wrong.
- Whether information considered by a person provides reasonable grounds for a suspicion depends on the source of the information and its context, drawing inferences as to what a reasonable person in the position of an independent observer would make of it.
- Information obtained later indicating that the grounds were not reasonable is not relevant to this assessment.

In Part 10, we include a list of 'disclosable matters' under the *Corporations Act*.

If you make a disclosure to your lawyer for the purposes of seeking legal advice, your disclosure will be protected.

Public Sector – PID

Under PID legislation, which covers public sector employees, a whistleblower will generally make a 'public interest disclosure' by reporting information to an eligible recipient that shows a public officer or public body has engaged in illegal activity or corrupt conduct, mismanagement or waste of public resources or conduct that causes substantial risk to health, safety or the environment. The exact grounds vary across the different PID regimes.

If you work for a company that provides services to a government entity then you may also be able to make a disclosure under the relevant public interest jurisdiction of the government entity.

A list of disclosable matters under the private sector *Corporations Act* and public sector PID legislation can be found in Part 10 of this Guide.

3.3 When will digital technology concerns be covered by the whistleblower protections?

Digital technology concerns are likely to arise in both the public and private sectors which means there is a possibility that your disclosure may be captured by either the private sector whistleblower laws or a PID scheme - depending on the organisation your report relates to. In most cases, this will be straightforward to determine, but if not we encourage you to seek legal advice.

Under most whistleblowing laws, a 'personal work-related grievance' that is not of a systemic or serious nature is not protected by law. So interpersonal disputes with colleagues are typically not covered.

4. Before blowing the whistle

4.1 Things to think about before blowing the whistle

Employment risks

Whistleblowing laws offer protection against reprisal or detriment to those who speak up. This means that it is unlawful for your employer to end your employment or cause other detriment to you because you made a disclosure.

However, despite these protections, it is a possibility that your employer may engage in unlawful behaviour. They may end your employment or take some other form of disciplinary action related to your whistleblowing disclosure. Whistleblowing laws often cannot prevent your employer from attempting to take detrimental action against you, but they do give you a right of action to seek preventative measures to stop your employer from taking detrimental action, or to seek compensation or damages for the retaliation. It is important to seek legal advice or support if you have any concerns about how to proceed. Note, this advice will be protected by legal professional privilege with the effect that the conversation is confidential.

Legal action

The act of making a whistleblower disclosure using a protected pathway is not illegal. As described above, the various private sector and PID legislation give eligible whistleblowers legal rights and protections to encourage people to come forward.

However, in Australia there have been instances where whistleblowers have faced legal action because their conduct has not been protected by whistleblowing laws. For example, where individuals have made an apparently unprotected disclosure to journalists and leaked government classified information or engaged in preparatory acts of whistleblowing which were allegedly unlawful. For this reason, we encourage you to seek legal advice on how to make a disclosure safely, following the pathways in the legislation, to lower these risks.

You must exercise caution about each of the steps you take to prevent any possible legal consequences down the track.

Personal assessment

Outside of the legal risks, blowing the whistle can also have potential social and emotional impacts. For example, there may be impacts to your reputation, career and emotional wellbeing, which should always be considered alongside any decision to disclose. While this is not a universal experience for all whistleblowers, you may wish to consider this before making a disclosure.

It might sound daunting, but making a personal assessment can help you think about speaking out regarding wrongdoing at your employer and plan ahead for what could be difficult terrain to navigate. The Signals Network's Personal Assessment tool (in Part 11) was devised to provide you with some practical questions to guide your thinking. Not all of them will apply in every case and you should not feel you need to answer them all before speaking out. These questions are a way to assess where you are and what you are willing to go through to speak out in order to develop your personal whistleblowing plan.

> *"I never wanted to be a whistleblower. But lives were in danger and I knew I had to do something. Blowing the whistle can be a daunting task even if you know it is the right thing to do . . . The best way to feel more confident is having the right support – from friends and family but also people who have been through the process before that can help you navigate through the legal, ethical, and personal decisions and issues you will face."*
>
> **Frances Haugen,** Facebook whistleblower

If you have made a disclosure and you are feeling anxious or stressed you should seek support. If your organisation has a whistleblower policy, they may have support available. You could also seek support through your organisation's Employee Assistance Program, if they have one, or speak to a private counsellor or psychologist.

Resources

- Personal assessment tool (provided by Signals Network) in Part 11.
- Lifeline Australia provides free, 24-hour telephone crisis support service in Australia. Go to https://www.lifeline.org.au/ or call 13 11 14.
- Beyond Blue has a free 24/7 webchat available, where you can speak to a counsellor.
- Find a psychologist in Australia near you at https://psychology.org.au/find-a-psychologist

4.2 Who should I speak to first?

We recommend that you seek legal advice before speaking to anyone or making a disclosure. Seeking legal advice is protected under most state, federal and private sector whistleblowing laws. Part 10 sets out a list of 'eligible recipients' who can receive whistleblower disclosures under the various private sector and PID laws.

Before your appointment with a legal advisor, you should look at your organisation's whistleblowing policy (if they have one) for nominated channels to report a concern to discuss with a lawyer. The policy should provide guidance as to who within the organisation you should raise your concerns with in the first instance. Not all organisations have a whistleblowing policy. You can still speak to a lawyer about the wrongdoing to receive advice on your circumstances.

4.3 I have signed an NDA: does this affect my ability to make a disclosure?

A Non-Disclosure Agreement (**NDA**) is a legal contract between two parties which prohibits the sharing of information deemed confidential. NDA clauses are often included in settlement deeds which may be signed after someone leaves their employment in contested circumstances.

Employers and employees are entitled to enter into a confidentiality agreement or NDA related to employment, provided both parties agree to the terms and the purpose of the agreement is not to conceal unlawful information.

In some circumstances, despite the clauses in the NDA, a person may still be able to disclose information relating to their whistleblower disclosure, including to regulators. However, a person should always seek legal advice before disclosing information that they think they are prevented from sharing because of the terms of their NDA. A lawyer will be able to provide specific advice having regard to the specific terms of the NDA. Consulting a lawyer about the terms of an NDA is not itself a breach of an NDA – you are entitled to seek advice and the lawyer is obliged to keep this advice confidential.

'Despite what your employer may want you to believe, NDAs cannot be used to "gag" you from seeking legal advice or reporting serious issues to the authorities. There are also ways to mitigate the risk of speaking out. Support groups like The Signals Network, or lawyers specialised in whistleblowing can help you map out a strategy that allows you to raise the alarm but stay protected.'

Jennifer Gibson - *Former Legal Director,* The Signals Network

4.4 Are there time limits?

There are no time limits imposed by the various private sector whistleblower laws regarding when to make a whistleblower disclosure. However, if you want to bring a claim about unlawful treatment as a whistleblower (e.g. you believe your employer has terminated you as a result of your disclosure or taken some other reprisal action against you, or disclosed your identity without your consent), there will be a time frame in which you must bring this claim. This time limit varies depending on the jurisdiction, or the whistleblowing law that applies to your disclosure. Under the *Corporations* Act, for private sector employees, you have six years to bring this claim from when the unlawful treatment occurred.

Under PID laws, the reportable conduct can have occurred before or after the laws commenced. However, in Tasmania, public interest disclosures cannot be made for issues that happened before 1 January 2001.

4.5 What evidence do I need?

You do not need to gather and provide evidence to prove a whistleblower disclosure. It is the role of your employer or a regulator to investigate the concern once it has been disclosed. An organisation's whistleblower policy may outline the key steps it will take after receiving a disclosure, including its investigation process and how they will keep you informed.

In some circumstances it is appropriate to provide supporting information when raising a concern. However, it is important to be cautious about how you collect this information. Downloading, forwarding or sending information relating to your employer via a personal email address, or accessing your employer's IT system without permission, could amount to misconduct and expose you to disciplinary action. More serious penalties can apply if you work for a government department and forward or take government information. You should think very carefully about gathering evidence and how evidence and other supporting documents are collected and seek legal advice before doing so. Recent case law has limited the scope of whistleblower protections to exclude preparatory conduct.

4.6 What if I have committed wrongdoing?

While an organisation cannot use your whistleblower report against you (for example, you cannot be terminated from your employment because you raised concerns) whistleblower laws do not give you immunity if you were involved in the misconduct you report.

However, if you are voluntarily reporting misconduct that you were involved in to a regulator (for example, ASIC) and are cooperative in doing so, your cooperation will likely be taken into account in any further action taken.

4.7 Can I be anonymous when making a disclosure?

You are able to make an anonymous disclosure under the *Corporations Act* and the PID legislation and receive whistleblower protections.

Those covered by the *Fair Work (Registered Organisations Act 2009* (Cth), *National Disability Insurance Scheme Act 2013* (Cth) or the *Aged Care Act 1997* (Cth) are not able to make protected anonymous disclosures.

An anonymous disclosure can, in some circumstances, limit the action an organisation can take in response to your disclosure or the protections an organisation can practically afford to you. For example, where you do not share your identity, it can make it difficult for organisations to conduct a complete investigation. It can also mean you cannot be contacted to provide further information about your concern. It also presents some challenges if you should wish to allege reprisal as a legal remedy to any detriment suffered as the organisation may say they did not know who made the disclosure and therefore did not target any person with detriment. In some jurisdictions, the pathways to an external disclosure, for example to a journalist or parliamentarian, are limited if the disclosure was anonymous.

Anonymous disclosures can still be valuable in uncovering misconduct if you do not feel comfortable identifying yourself and organisations can still take steps to address your concerns. Alternatively, sometimes it may be possible to blow the whistle via your legal representatives, to protect your identity while still permitting further conduct with the employer or regulator.

5. Who can I make a disclosure to?

For your disclosure to be protected by law, it must be made to the right person or organisation.

It's often assumed that whistleblowing is about making disclosures to the media, but in order to be eligible for certain legal protections, you are often required to make internal disclosures first, and to specific people. It is good practice to keep notes of these conversations, should you need to rely on legal protections later.

Refer to your company's whistleblower policy (if one exists) for the nominated channels to report a concern. In most cases, the simplest, safest and most efficient way is to raise the concern directly with your organisation, in line with its whistleblower policy.

If your organisation does not have a whistleblowing policy, you should make your disclosure to an 'eligible recipient' at law - see below - or seek legal advice.

5.1 Who can I make a disclosure to under law?

Private sector whistleblower laws

Part 10 contains a list of 'eligible recipients' who can receive whistleblower reports under private sector whistleblower laws.

It is important to keep in mind that you might feel inclined, or your organisation may encourage you to raise concerns with your immediate supervisor or someone in Human Resources as a first step. However, doing so can mean you do not qualify for the whistleblower protections unless your immediate supervisor or the Human Resources personnel is an 'eligible recipient' at law, or otherwise nominated in your organisation's whistleblower policy to receive disclosures.

You should disclose your concerns to an 'eligible recipient' under the relevant legislation, or to a person nominated to receive whistleblower reports in your organisation's whistleblower policy.

PID laws

The PID laws also identify the people and bodies that you can make a public interest disclosure to.

Part 10 sets out a list of the people and bodies who can receive whistleblower reports under PID laws. The list is not exhaustive of all of the requirements under each PID Act - you should check the PID laws in your state or territory and seek legal advice on who to make your disclosure to if it is not clear.

6. Can I go to the media or a politician?

6.1 When should I go to the media or to a member of Parliament about my concern?

Many whistleblowing laws recognise the importance of public accountability, with legal protections for speaking up to journalists, politicians or civil society groups. However, these protections are limited and narrow. Under both public and private sector whistleblowing laws, you may not be protected from any reprisal action if you first make a disclosure to a parliamentarian or journalist, except in extreme circumstances. This means you could face legal risk or impact to your employment, and you may not have any remedies available to you at law. In limited circumstances, certain public interest disclosures or 'emergency' disclosures that are made to journalists or parliamentarians are protected by whistleblowing laws.

The requirements under law must be strictly followed for the protections to apply. Generally, there are time limits that will apply, where you must wait a certain period of time between making a disclosure internally or to a regulator before you can make an external disclosure. The laws on whistleblowing are complex, and we recommend you seek legal advice before making a public disclosure, even if you feel it is appropriate to disclose your concerns to the media or a member of Parliament.

6.2 What is parliamentary privilege?

Parliamentary privilege is a legal right that protects the business of parliament. Parliamentary privilege can extend to concerns brought to a member of Parliament from a whistleblower. Where a whistleblower brings matters concerning a public interest to the attention of a member, the member may choose to raise the concern in Parliament. The application of parliamentary privilege is complex; specialist advice should be sought before proceeding.

6.3 'Public interest disclosures' under the *Corporations Act*

The first steps of a disclosure pathway under the *Corporations Act* are to make an internal disclosure or disclosure to the regulator. In some circumstances, you can make a disclosure to a journalist or parliamentarian and be protected. The *Corporations Act* refers to this as a 'public interest disclosure'. To make a public interest disclosure:

A. You must have **previously made a protected disclosure to ASIC or APRA**;

B. at least 90 days' must have passed since your protected disclosure was made, and **you do not have reasonable grounds** to believe that action to address your concerns is being or has been taken; and

C. you **must have reasonable grounds** to believe that reporting your concerns to a journalist or parliamentarian would be in the public interest; and

D. you must give **written notice to whoever the internal disclosure was made to, giving sufficient information to identify your earlier report and stating your intention to make a public interest disclosure**. For example, this may include contacting the ASIC or APRA officer who considered your initial concerns; and

E. the extent of information disclosed in your public interest disclosure should be no greater than is necessary to inform the recipient about your concerns.

6.4 Emergency disclosures under the *Corporations Act*

In some instances where there is a real risk to the danger to the health or safety of one or more persons or to the natural environment, an individual does not need to wait 90 days before proceeding to make further disclosures. A disclosure will qualify as an "emergency disclosure" under the *Corporations Act* where the disclosure has **reasonable grounds** to believe that the information concerns a **substantial** and **imminent** danger to the health or safety of one of more persons or to the natural environment.

In order to qualify for protection as an 'emergency disclosure' under the *Corporations Act*, you need to have previously made a disclosure that qualifies for protection which can be identified in the course of making an emergency disclosure.

Examples of emergency disclosures in a technology context may include:

- During routine testing, a technical employee at a new 'chatbot' company popular with under-18 users notices a vulnerability where chatbots are encouraging users into self-harm and related harmful ideation. The employee believes vulnerable users could be immediately at risk.
- An employee of a company collecting and processing sensitive health data realises that an error has caused some information to be readily identifiable, meaning that a significant amount of patients' health records could be linked to them, exposed and stolen.
- A digital advertising company comes across a type of 'audience segment' available for sale that it believes would uniquely and exclusively identify Australian national security personnel.

As with public interest disclosures under the *Corporations Act*, if you proceed to make an emergency disclosure to a journalist or parliamentarian, the extent of information disclosed should be no greater than is necessary to inform the recipient about your concerns.

Public sector laws

Under the public sector PID legislation, you can make a disclosure to a parliamentarian or journalists in particular circumstances. This varies depending on which PID law applies (i.e. whether it is the federal PID legislation or a state or territory).

For example, under the federal public sector PID legislation, if the conduct you are making a disclosure about poses a **substantial and imminent threat** to health or safety, or **the environment**, you may be able to make an "emergency disclosure" of the information. You must:

- have already made an internal disclosure through the pathways available; OR
- there must be exceptional circumstances for skipping this step.

An emergency disclosure can be made to any person except a foreign public official, for example a journalist, a parliamentarian or a civil society group. The disclosure must not contain intelligence information, and the extent of the information disclosed should be no greater than necessary to inform the recipient of your concerns.

You should refer to the relevant PID legislation for your government department for guidance on the steps you should take if you want to make a disclosure to a parliamentarian or the media. Disclosures to parliamentarians and journalists are not provided for under all PID legislation.

7. Protections for whistleblowers

7.1 How am I protected as a whistleblower?

If correct disclosure pathways are followed so that an individual making a disclosure is eligible to receive protections (i.e. an eligible whistleblower), it is unlawful to cause detriment, reprisal or harm to the eligible whistleblower.

These words are used interchangeably but they are what is known as 'victimisation'. It is unlawful for an organisation to victimise and cause detriment to an eligible whistleblower. This means that eligible whistleblowers who experience victimisation because of their protected disclosure can pursue a legal remedy in court.

Why do these protections exist?

Eligible whistleblowers are given certain protections under the law that are designed to encourage them to come forward to report misconduct without fear of retribution or personal detriment.

Confidentiality

Whistleblower protections under both the private sector laws and public sector PID legislation require a recipient of a whistleblower disclosure to keep the identity of the whistleblower confidential. You are provided with confidentiality protections which restrict certain information from being disclosed directly or indirectly due to your report. The information that is protected and anything not covered varies across the different private and public sector laws.

For example, under the *Corporations Act*, it is illegal to disclose the identity of a whistleblower, including information that is likely to lead to their identification, without their consent (unless an exception applies). This means recipients of your disclosures **must keep your identity confidential to the fullest extent possible.**

Under all other private sector whistleblower legislation and public sector PID legislation, your identity must be kept confidential when you make a protected disclosure.

Where you do not consent to your identity being disclosed to people involved in the investigation, a full investigation may not be possible.

Non-victimisation

There are protections which prevent whistleblowers from suffering detriment because they made a protected disclosure. These protections vary across the private sector laws in terms of how 'detriment' is defined. Generally, it is against the law to take or threaten to take any detrimental action against a whistleblower because a person believes or suspects that the whistleblower has or could make a disclosure that qualifies for whistleblower protections.

Examples of reprisal that will be included in the definition of detriment across the various laws include: dismissal, injuring an employee in their employment, altering an employee's position or duties to their disadvantage, harassment or intimidation, causing harm or injury, and numerous types of damage (property, reputational, financial).

You should consult the relevant legislation if you have made a whistleblower protected disclosure and believe you are suffering detriment as a result.

Importantly, under all whistleblower laws, the detriment suffered **must be the result of the actual or suspected whistleblower disclosure**.

7.2 What should I do if I suffer detriment?

Where you believe your protections around confidentiality and/or non-victimisation have been breached or you otherwise believe negative action has been taken against you, as an initial starting point you should obtain legal advice and/or discuss the concerns with the organisation's Whistleblower Protection Officer (if one exists). You should also refer to your organisation's whistleblower policy (if they have one) for guidance on who to speak to and who to seek support from.

If your organisation does not have a Whistleblower Protection Officer appointed or you are unable to easily identify who you could speak to:

- the person to whom you made your disclosure originally, or another person within the organisation that you trust;
- if your organisation has engaged a third-party whistleblower service provider, you may refer to these services; or
- you may wish to escalate your concerns to senior management or a member of the Board of your organisation (if appropriate).

Where your concerns cannot be resolved easily or the detriment suffered is causing distress, risk to employment or loss of employment, we recommend you seek independent legal advice immediately.

7.3 Can I take the organisation to court if I suffer detriment?

Yes.

If you suffer detriment because you are an eligible whistleblower, you can generally seek compensation and other remedies through the courts if you suffer loss, damage or injury because of the disclosure. Under the *Corporations Act*, for example, this includes if the organisation does not take reasonable precautions to prevent the detrimental action against you. You should seek legal advice if you are considering seeking these remedies as there may be time limits which apply.

8. Checklist of considerations when raising digital technology concerns

Blowing the whistle can be a *stressful process.*

The following checklist provides some important things to consider, that you might want to discuss further with a lawyer.

What outcome are you hoping for by blowing the whistle?

The best outcome is that an organisation takes the disclosure seriously, investigates in a timely manner, corrects the behaviour, discloses any wrongdoing and no detriment is caused to the discloser.

Do you have a support network to help you?

Blowing the whistle can be a difficult decision and can impact your personal and professional life, and particularly your health and wellbeing. You should assess whether you have appropriate supports in place before deciding to make a disclosure and seek help from a professional when needed.

Do you think there is a risk you will be victimised?

Consider how your organisation has treated whistleblowers in the past and consider that in your disclosure steps and strategy. If your concerns are shared by others, can this be raised collectively? Raising concerns together can help lower the risk of victimisation against you individually.

Consider remaining anonymous

You may be able to remain anonymous when making a disclosure. If you are concerned you may be victimised for making a whistleblower disclosure, or otherwise do not want your identity to be known, consider raising your concern anonymously.

Avoid acting as an investigator

Your role as a whistleblower is to report your concerns, not to investigate them. An investigation conducted by a whistleblower could undermine a formal investigation later undertaken by your employer and could contain risk.

Have you followed your organisation's policies/procedures?

As outlined in this Guide, one of the first steps you should take when making a whistleblower disclosure is to check your organisation's whistleblower policy and follow the procedure to make a disclosure. Your concern may be addressed more quickly if you raise your concerns to the right person and will also help ensure your disclosure is protected.

Provide clear information and stay professional

Make sure the information you provide in your disclosure is clear and provides support for your reported concern. Check that your concerns are raised professionally and avoid making personal criticisms of others - focus on the facts.

Ask what the next steps are and timeframes

If you decide to make a disclosure, ask your organisation what the next steps are and for timeframes of any proposed action to be taken.

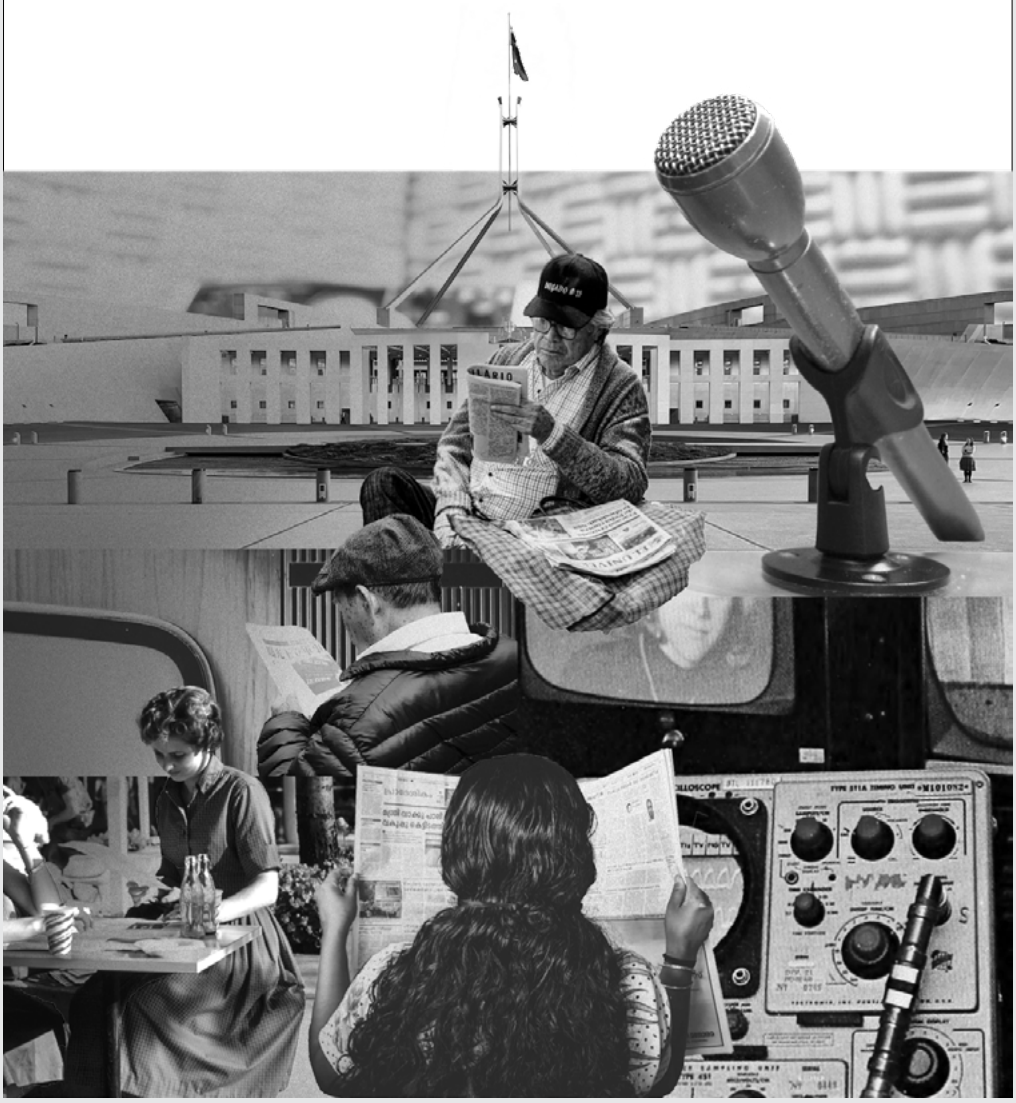
Make a private note

Make a private note of what you raised, how you raised it, when and to whom, especially if you decide to raise your concerns verbally rather than in writing. Keep a note of any actions taken and any subsequent treatment towards you that you feel is negative.

9. Case Studies

The following case studies are prepared as hypothetical examples. They indicate the breadth of possible issues and situations for digital technology concerns.

They are indicative only and are not meant to represent real scenarios.



A. **Private sector** – large international digital platform

Gary works as a senior product manager in the global headquarters of an American digital platform company. He becomes increasingly concerned with the decisions being made to alter the 'news feeds' of users around the world, including in Australia, where a new feature is being tested through his company's Australian subsidiary. Gary is concerned about the deterioration of the online news environment in these trial markets and has been working closely with the Australian subsidiary as part of its tests. Gary has also been part of an internal working group where the company has been reviewing in-house research and refining their policies as they relate to young girls and disordered eating risks. Gary believes the company is ignoring warnings from the in-house research and continuing to allow algorithms and features operate in ways that are causing harm to young girls' health. Gary also noticed that some of the press releases about new safety features for teens were describing features that were not working in Australia, despite these announcements getting reported extensively in the Australian media.

Is Gary able to make a protected disclosure?

Although Gary is a non-resident and non-citizen of Australia, whistleblower protections and pathways may be available to him under the *Corporations Act*. His company's Australian subsidiary would likely be a regulated entity under the *Corporations Act*, and these provisions have extra-territorial effect. Gary's work with the Australian subsidiary might therefore qualify him as an eligible whistleblower, as someone providing services to the subsidiary. The wrongdoing at the global holding company would be captured as wrongdoing by a related body corporate of the Australian legal entity.

Could Gary make an emergency disclosure under the Corporations Act?

The conduct Gary is concerned about might be misleading and deceptive conduct, prohibited under the *Australian Consumer Law*. To qualify for protection as an 'emergency disclosure' under the *Corporations Act*, a person needs to have previously made a protected disclosure to ASIC. Gary would need to write to ASIC informing them that he intends to make an emergency disclosure. He could then approach an Australian parliamentarian under parliamentary privilege and make an emergency disclosure. He would need to be satisfied that the threshold for 'substantial and imminent danger' to health and safety is met. While this question is untested in the context of a digital platform company, either the news distribution issue or the disordering eating algorithms issue may be sufficient to meet the test of 'substantial and imminent dangers to the health or safety of one or more persons or to the natural environment'.

B. **Private sector** – Australian data firm

Su-Lin works as a data analyst in one of Australia's biggest 'data broker' firms. Su-Lin believes in the power of data and has made it the focus of her career, but she is increasingly worried about the datasets entering the company. Some of the datasets are easily identifiable to a person and are sensitive in nature. Su-Lin also has concerns about who the data is getting sold to, as she believes overseas scammers are purchasing some datasets to make their scams more sophisticated. After raising these concerns informally with a colleague, an in-house lawyer at the company, Su-Lin believes that the company may be acting unlawfully by recklessly on-selling Australians' data to criminal actors. However, Su-Lin is deeply worried about her employment prospects should she speak up.

What can Su-Lin do next?

In the first instance, Su-Lin should consult her employer's whistleblowing policy, if they have one, and make a disclosure internally. As her company will be covered by the *Corporations Act*, the whistleblower pathways and protections will be available to Su-Lin. A current employee of the company that the disclosure is about is an eligible whistleblower. Su-Lin's disclosure relates to the potential misconduct of the company, namely that they do not have sufficient protections in place to ensure that the data they hold is not vulnerable to being sold to scammers. Su-Lin is an eligible whistleblower for the purposes of the *Corporations Act*. For the disclosure to be protected, the *Corporations Act* provides that Su-Lin must have reasonable grounds to suspect the information she is disclosing about the company concerns misconduct or an improper state of affairs and must make her disclosure to an 'eligible recipient'. This is usually a designated person within the organisation, ASIC, or another proscribed regulator. At the time of writing, there are no protected pathways under the *Corporations Act* to make a disclosure to any regulator other than ASIC or APRA. If Su-Lin has a reasonable basis for her concerns that the company is acting unlawfully, that would probably constitute misconduct or an improper state of affairs.

If Su-Lin raises her concerns to ASIC, and nothing is done, after 90 days Su-Lin may have the ability to escalate her concerns to a journalist or a politician. However, as these external disclosures provisions are quite complex, to ensure she is protected, Su-Lin may wish to seek legal advice before proceeding.

C. **Public sector** – State government

Zephyr is a policy officer working at the Victorian Department of Justice and Community Safety. Their team has been involved in procuring technology from a company that claims to bring advanced artificial intelligence to support law enforcement objectives. Zephyr has been concerned that the tech is, at best, unreliable, and at worst, harmful to Victorians. Zephyr knows a bit about some of these algorithms work, and reckons there's some risks in the underlying systems that have been ignored or missed by the higher-ups. Zephyr runs some of their own experiments on the software and mentions their concerns to their supervisor in-person, who doesn't seem to understand. Zephyr then follows up over email. The supervisor drops by their desk and says 'don't write to me about those sorts of techy tin-foil hat issues again, the Minister is all-in on innovation and it's your job to make that happen. I don't care if a few kids get racially profiled, the cops do that every day without all this AI stuff anyway'.

Is Zephyr able to make a protected disclosure?

Any person can make a disclosure about 'improper conduct' perpetrated by a public officer or public body in Victoria and be protected by the *Public Interest Disclosure Act 2012* (Vic). Improper conduct can include an intentional or reckless breach of public trust and a substantial risk to the health or safety of one or more persons. Zephyr could potentially characterise the public body's decision to routinely ignore serious risks to the public from the new software as improper conduct, although the situation may need to further deteriorate to encourage this assessment. However, to make a protected disclosure, Zephyr need only have a reasonable belief that the information shows improper conduct. As such, they are likely to still be protected in making a disclosure to an eligible recipient, so far as they reasonably believe that the information shows improper conduct, such as a reckless breach of public trust or serious professional misconduct on part of their supervisor.

Was Zephyr's email to their supervisor a protected disclosure?

A supervisor is any public officer responsible for supervising or managing the discloser, which in this scenario, includes Zephyr's supervisor. Zephyr's email would need to provide information that shows or tends to show (or that Zephyr reasonably believes to show) that a person, public officer, or public body has engaged, is engaging, or proposes to engage in improper conduct. Zephyr's email may meet the threshold of improper conduct, however it is not certain where the disclosure has not been treated as a public interest disclosure or 'PID' by the recipient.

What was Zephyr's supervisor required to do with the information?

Under the Act, supervisors must be aware of how the law operates, and how to respond to potential public interest disclosures. Where a supervisor receives information from a public official that they reasonably believe contains disclosable conduct, they are required to refer the information to an 'authorised officer' and inform the discloser of the process for managing the disclosure.

Zephyr's supervisor should have:

- informed them that their disclosure could be treated as an internal disclosure;
- explained the next steps in the PID process, including the referral of the disclosure to an authorized officer and the investigation process;
- advised Zephyr about the circumstances in which a disclosure must be referred to an agency, or other person or body; and explained the protections that may be available to Zephyr.

10. Summary of Australian Whistleblowing Laws

Who can be an eligible whistleblower?

PRIVATE SECTOR whistleblower laws

Legislation	**A whistleblower must be a current or former:**
Corporations Act 2001 (Cth)	› Employee of the relevant company or a related entity of that company; › Officer of the relevant company or a related entity of that company, for example, a company director or secretary; › Person who supplies goods or services to the company or a related entity of that company the disclosure is about (i.e. a contractor or volunteer); › Individual who is an associate of the company or a related entity of that company; › Trustee, custodian or investment manager of a superannuation entity; or › Spouse, relative or dependent of one of the people referred to above, or a dependent of such an individual's spouse.
Tax Administration Act 1953 (Cth)	› An officer of the entity; › An employee of the entity; › An individual who supplies services or goods to the entity (whether paid or unpaid); › An employee of a person that supplies services or goods to the entity (whether paid or unpaid); › An individual who is an associate of the entity; › A spouse or child of one of the people referred to above; or › A dependent of one of the individual's referred to above, or a dependent of such an individual's spouse.
Fair Work (Registered Organisations) Act 2009 (Cth)	› An officer or former officer of the registered organisation, or one of its branches; › An employee or former employee of the registered organisation, or one of its branches; › A member or former member of the registered organisation, or one of its branches; › A person who has (or had) a contract for the supply of services or goods to, or any other transaction with, an organisation, or one of its branches (or an officer, former officer, employee or former employee of this person); › A person who has (or had) a contract for the supply of services or goods to, or any other transaction, an officer or employee of an organisation, or one if its branches, who is (or was) acting on behalf of the organisation or branch (or a an officer, former officer, employee or former employee of this person); or › A lawyer on behalf of a discloser in one of the above categories.

Who can be an eligible whistleblower?

PUBLIC SECTOR whistleblower laws

Legislation	**A whistleblower must be:**
Public Interest Disclosure Act 2013 (Cth)	› A current or former **public official*** at the time of disclosure, including a contracted service provider to the Commonwealth or an employee of a contracted service provider. *Under the *Public Interest Disclosure Act 2013* (Cth), a public official includes an APS employee in a Department, a member of staff of an agency other than a Department (including an APS employee in the agency), a Secretary of a Department, the principal officer of an agency other than a Department, an individual who constitutes a prescribed authority, a member of a prescribed authority (other than a court), a director of a Commonwealth company, a member of the Defence Force, or a cadet, officer or instructor in the Australian Defence Force Cadets, an Australian Public Service (**APS**) employee in a Department or a staff member of an agency, a Parliamentary service employee, an individual who is employed by the Commonwealth other than as an APS employee and performs duties for an agency, a statutory officeholder, an individual who is a contracted service provider for a Commonwealth contract, an individual who is an officer or employee of a contracted service provider for a Commonwealth contract provides services for the purposes (whether direct or indirect) of the Commonwealth contract, an individual (other than a statutory officeholder or an official of a registered industrial organisation) who exercises powers, or performs functions under a law of the Commonwealth, Norfolk Island, the Territory of Christmas Island or the Territory of Cocos (Keeling Islands) or the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.
Public Interest Disclosures Act 2022 (NSW)	› A **public official*** at the time of disclosure, for mandatory and voluntary public interest disclosures. Members of Parliament cannot make voluntary public interest disclosures. › A witness public interest disclosure is made where a person (i.e not only a public official as defined) discloses information during an investigation of serious wrongdoing following a request or requirement of the investigator. *Under the *Public Interest Disclosures Act 2022* (NSW), a public official means one or more of the following: a person employed in or by an agency or otherwise in the service of an agency; a person having public official functions or acting in a public official capacity; an individual in the service of the Crown, a statutory officer; a person providing services or exercising functions on behalf of an agency (i.e. a contractor, subcontractor or volunteer); an employer, partner or officer of an entity involved in providing services on behalf of an agency, a judicial officer; a member of Parliament (i.e. a Minister) and a person employed under the *Members of Parliament Staff Act 2013* (NSW).

Legislation	A whistleblower must be:
Public Interest Disclosure Act 2018 (SA)	› A **public officer*** who makes an appropriate disclosure of public administration information. › Any person, where the person makes an appropriate disclosure of public administration information. *Under the *Public Interest Disclosure Act 2018* (SA), a 'public officer' has the same meaning as that under the *Independent Commission Against Corruption Act 2012* (SA), including a Governor, a person appointed to an office by the Governor, a Member, officer or person under the separate control of the President of the Legislative Council, a Member or officer of the House of Assembly, or a person under the separate control of the Speaker of the House of Assembly, a member of the joint parliamentary service, a judicial officer, the principal officer of a judicial body, a judicial officer that constitutes a judicial body, a member of staff of the State Courts Administration Council, a person who constitutes a statutory authority, or who is a statutory office holder, a member, officer or employee of a statutory authority, a member, officer or employee of a local government authority, the Local Government Association of South Australia (or an officer or employee), the chief executive or an employee of an administrative unit of the Public Service, a police officer or police security officer, an officer or employee appointed by the Chief Executive under the *Education and Children's Services Act 2019,* a person appointed by the Premier under the *Public Sector Act 2009,* a person appointed by the *Minister under the Public Sector Act 2009,* any other public sector employee, a person to whom a function or power of a public authority or a public officer is delegated in accordance with an Act, a person who is, in accordance with an Act, assisting a public officer in the enforcement of the Act, a person performing contract work for a public authority or the Crown or a person declared by regulation to be a public officer.
Public Interest Disclosure Act 2002 (Tas)	› A **public officer***, contractor or subcontractor, or an employee of a contractor who has entered into a contract with a **public body**** for the supply of goods or services. › Any person (if a disclosure about improper conduct or detrimental action under Part 2 of the *Public Interest Disclosure Act 2002* (Tas)) if the disclosure is considered to be in the public interest. *Under the *Public Interest Disclosures Act 2002* (Tas), a public officer includes a member of Parliament, a councillor, a member, officer or employee of a public body, an employee of a council, any person performing functions under the *Parliamentary Privilege Act 1898*, a person employed in an office of a Minister, Parliamentary Secretary or other Member of Parliament, any person performing functions under the *Governor of Tasmania Act 1982* or a person appointed to an office by the Governor or a Minister under an Act. **Under the *Public Interest Disclosure Act 2002* (Tas) public bodies include the Parliament of Tasmania, a State Service Agency, the Police Service, a council, a Government Business Enterprise, a State-owned Company, a council-owned company; the University of Tasmania; a body or authority, whether incorporated or not, whose members are appointed by the Governor or a Minister or any other prescribed body or authority, whether incorporated or not to which any money is paid by way of appropriation from the Public Account or over which the Government or a Minister exercise control.

Legislation	A whistleblower must be:
Public Interest Disclosures Act 2010 (Qld)	› A **public officer*** of a **public sector entity**** at the time of the disclosure who has information about: › The conduct of another person that could, if proved be corrupt conduct or maladministration that adversely affects a person's interests in a substantial and specific way; › A substantial misuse of public resources (other than an alleged misuse based on mere disagreement over policy that may properly be adopted about amounts, purposes or priorities of expenditure); › A substantial and specific danger to public health or safety; or › A substantial and specific danger to the environment. › Any person, if they have information about: › A substantial and specific danger to the health or safety of a person with a disability; › The commission of an offence related to specific provisions concerning substantial and specific danger to the environment; › A contravention of a condition imposed under specific provisions related to substantial and specific danger to the environment; or › The conduct of another person that if proved, could be a reprisal. *Under the *Public Interest Disclosures Act 2010* (Qld), a **public officer** means an employee, member or officer of a public sector entity, as well as the Minister responsible for administration of a department, a member of a school council, a Ministerial staff member employed in the office of a Minister or an Assistant Minister. **Under the *Public Interest Disclosures Act 2010* (Qld), a **public sector entity** means a committee of the Legislative Assembly, the parliamentary service, a court or tribunal, the administrative office attached to a court or tribunal, the Executive Council, a department, a local government, a registered higher education provider or TAFE Queensland, an entity established under an Act or under State or local government authorisation for a public, State or local government purpose or an entity prescribed under a regulation assisted by public funds.
Independent Commissioner Against Corruption Act 2017 (NT)	› Any person, being an individual.
Public Interest Disclosures Act 2012 (Vic)	› A natural person.
Public Interest Disclosure Act 2003 (WA)	› Any person.
Public Interest Disclosure Act 2012 (ACT)	› Any person.

Who is an eligible recipient of a whistleblower disclosure?

PRIVATE SECTOR whistleblower laws

Legislation	Who can I disclose to?
Corporations Act 2001 (Cth)	› Australian Securities and Investments Commission (ASIC); › Australian Prudential Regulatory Authority (APRA); › An internal or external auditor; › A legal practitioner (to obtain legal advice about the disclosure); › A trustee (if the organisation is a superannuation entity); › An officer (for example a director or company secretary) or senior manager* of the organisation; › An actuary of the organisation; › A person authorised by the organisation to take disclosures that qualify for protection under the *Corporations Act*. *Under the *Corporations Act*, a senior manager means a person who participates in making decisions that affect the whole or a substantial part of the business or a person who has the capacity to significantly affect the company's financial standing, for example, a senior executive of the company such as a Chief Executive Officer, Chief Financial Officer or a Chief Operating Officer.
Tax Administration Act 1953 (Cth)	› An auditor, or a member of an audit team conducting an audit, of the entity. › A registered tax agent or BAS agent (within the meaning of the Tax Agent Services Act 2009) who provides tax agent services or BAS services to the entity. › A person authorised by the entity to receive disclosures that may qualify for protection under the Act. › A person or body prescribed for the purposes of the Act in relation to the entity. › If the entity is a body corporate, each of the following is an eligible recipient in relation to the entity: › A director, secretary or senior manager of the body corporate. › Any other employee or officer of the body corporate who has functions or duties that relate to the tax affairs of the body corporate. › If the entity is a trust, each of the following is an eligible recipient in relation to the entity: › A trustee of the trust. › A person authorised by a trustee of the trust to receive disclosures that may qualify for protection under the Act. › If the entity is a partnership, each of the following is an eligible recipient in relation to the entity: › a partner in the partnership; › a person authorised by a partner in the partnership to receive disclosures that may qualify for protection under the Act.

Legislation	Who can I disclose to?
Fair Work (Registered Organisations) Act 2009 (Cth)	› The General Manager. › An FWC Member or a member of staff of the FWC. › A member of the staff of the Office of the Fair Work Ombudsman.

Who is an eligible recipient of a whistleblower disclosure?

PUBLIC SECTOR whistleblower laws

Legislation	Who can I disclose to?
Public Interest Disclosure Act 2013 (Cth)	› An authorised internal recipient; › A supervisor of the discloser; › Any person other than a foreign public official; › An Australian legal practitioner;
Public Interest Disclosures Act 2022 (NSW)	Voluntary public interest disclosures must be made to the head of an agency, another disclosure officer for an agency, a manager of the person making the disclosure, a Minister or a member of a Minister's staff (if in writing), or a member of Parliament or a journalist. Nb. The *Public Interest Disclosures Act 2022* (NSW) does not set out prescribed recipients for mandatory public interest disclosures or witness public interest disclosure.

Legislation	Who can I disclose to?
Public Interest Disclosure Act 2018 (SA)	› A supervisor/person taken to be responsible for the management/supervision of a public officer*, or to the relevant responsible officer, where the information relates to a public officer; › The Commissioner for Public Sector Employment, or the responsible officer for the relevant public sector agency, where the information relates to a public sector agency** or employee; › The Ombudsman, where the information relates to an agency to which the *Ombudsman Act 1972* (SA) applies; › A member, officer or employee of a particular council, where the information relates to a location within the area of a particular council established under the *Local Government Act 1999* (SA); › The Environmental Protection Authority, where the information relates to a risk to the environment; › The Auditor-General, where the information relates to an irregular and unauthorised use of public money or substantial mismanagement of public resources; › A member of the police force, where the information relates to an offence, or suspected offence; › The Judicial Conduct Commissioner, where the information relates to a judicial officer; › The Presiding Officer of the relevant House of Parliament, where the information relates to a member of Parliament; › An authority declared by regulations to be a relevant authority in relation to information, where the information relates to a person or a matter of a prescribed class; › Generally speaking, a Minister of the Crown, Office of Public Integrity, or any other prescribed person of a prescribed class under the legislation. *As defined above. **Under the *Public Interest Disclosure Act 2018* (SA), a public sector agency has the same meaning as that under the *Public Sector Act 2009* (SA), including a Minister, a chief executive of an administrative unit; an administrative unit, an employing authority, any other agency or instrumentality of the Crown, a body corporate comprised of persons, or with a governing body comprised of persons, a majority of whom are appointed by the Governor, a Minister or an agency or instrumentality of the Crown or subject to control or direction by a Minister; or a person or body declared to be a public sector agency (or a subsidiary of a Minister or a person or body of that agency).
Public Interest Disclosures Act 2002 (Tas)	› The Commissioner of Police, where the disclosure relates to a member of the Police Service; › The Ombudsman, where the disclosure relates to the Commissioner of Police; › The President of the Legislative Council, where the disclosure relates to a member of Parliament if the member is a member of the Legislative Council; or the Speaker of the House of Assembly, if the member is a member of the House of Assembly; › The Ombudsman, where the disclosure relates to a councillor; › The Ombudsman or the Integrity Commission, where the disclosure relates to persons employed under the *Parliamentary Privilege Act 1898* (Tas); › The Chairman of the Public Accounts Committee, where the disclosure relates to the Auditor-General; › The Joint Committee, where the disclosure relates to the Ombudsman; › The Ombudsman, where the disclosure relates to a person employed in an office of a Minister, Parliamentary Secretary or other Member of Parliament.

Legislation	Who can I disclose to?
Public Interest Disclosure Act 2010 (Qld)	› Chief judicial officer › A member of Legislative Assembly, unless the disclosure relates to a judicial officer; › A public sector entity*, if the disclosure relates to the conduct of the entity or any of its public officers**, anything the entity has a power to investigate or remedy or where the conduct of another person amount to a reprisal that relates to a previous disclosure, unless the disclosure relates to a judicial officer, the chief judicial officer of the relevant court or tribunal, or to the Crime and Corruption Commission if the disclosure relates to a judicial officer. *As defined above. ** As defined above.
Independent Commissioner Against Corruption Act 2017 (NT)	› The Independent Commissioner Against Corruption (ICAC) or the ICAC's Office; › The Inspector or a member of Inspector staff, where the information relates to the ICAC, the ICAC's Office or a member of ICAC staff; › The Ombudsman or the Ombudsman's Office; › The Auditor-General or the Auditor-General's Office; › The Health and Community Complaints Commissioner or a staff member of the Commissioner; › The Children's Commissioner; › The Environment Protection Authority; › The Commissioner of Police, where the information relates to a police officer; › The Speaker, where the information relates to a member of the Legislative Assembly other than the Speaker; › The Deputy Speaker, where the information relates to the Speaker; › The next Senior Supreme Court Judge, if the information relates to the Chief Justice; › The Chief Justice, if the information relates to a Supreme Court Judge or to the Chief Judge, other than the Chief Justice; › The Chief Judge, if the information relates to a Local Court Judge other than the Chief Judge; › The Electoral Commissioner, if the information relates to a contravention of the *Electoral Act 2004* (NT); › The entity with responsibility for the management and control of the public body, or a nominated recipient for the public body, if the information relates to an employee or officer of a public body.

Legislation	Who can I disclose to?
Public Interest Disclosures Act 2012 (Vic)	› The Independent Broad-based Anti-corruption Commission (IBAC); › The Ombudsman; › The Victorian Inspectorate; › A public service body* if the disclosure relates to the conduct of the public service body or of a member, officer or employee of that body; › A public officer* if the disclosure relates to an employee of, or any person otherwise engaged by, or acting on behalf of, or acting as a deputy or delegate of that public officer; › A Council if the disclosure relates to the conduct of a Council or of a member, officer, or employee of a Council; › A speaker of the Legislative Assembly, if the disclosure relates to a member of the Legislative Assembly *Under the *Public Interest Disclosures Act 2012* (Vic), a public service body includes a Department, an Administrative Office (i.e an administrative office in relation to a Department) or the Victorian Public Sector Commission. **Under the *Public Interest Disclosures Act 2012* (Vic), a public officer includes an IBAC Officer, a Victorian Inspectorate Officer, a Public Interest Monitor (i.e the Principal and Deputy Public Interest Monitors as appointed under the *Public Interest Monitor Act v* (Vic)).
Public Interest Disclosure Act 2003 (WA)	› A public officer/ person responsible for receiving PIDs › The police or the Corruption and Crime Commission, where the information relates to an act or omission that is an offence; › The Auditor General, where the information relates to a substantial unauthorised or irregular use of, or substantial mismanagement of public resources; › A Parliamentary Commissioner for Administrative Investigations, where the information relates to a matter of administration that can be investigated under section 14 of the *Parliamentary Commissioner Act 1971* (WA); › The Commissioner of Police, or the Corruption and Crime Commission, where the information relates to a person who holds an appointment under Parts I, II, IIIA or IIIB of the *Police Act 1892* (WA); › The Chief Justice, where the information relates to a judicial officer; › The Presiding Officer of the House of Parliament to which the member belongs, where the information relates to a member of either House of Parliament; › The Commissioner or the Parliamentary Commissioner, where the information relates to a public officer (other than a member of Parliament, a Minister of the Crown, a judicial officer or an officer referred to above to the *Parliamentary Commissioner Act 1971* (WA)).

Legislation	Who can I disclose to?
Public Interest Disclosure Act 2012 (ACT)	› A disclosure officer; › A Minister; › If the person is a public official* for a public sector entity**; › A person who, directly or indirectly, supervises or manages the person, or for a public sector entity that has a governing board - a member of the board, or a public official of the entity who has the function of receiving information of the kind being disclosed or taking action in relation to that kind of information. *Under the *Public Interest Disclosure Act 2012* (ACT), a public official includes a current or former employee of the public sector entity, or a contractor, employee of a contractor or volunteer exercising a function of the public sector entity. **Under *Public Interest Disclosure Act 2012* (ACT), a public sector entity includes an ACTPS entity (including the public service, a territory authority, a territory-owned corporation, a subsidiary of a territory-owned corporation, a territory instrumentality or a statutory office-holder), a Legislative Assembly entity (including a member of the Legislative Assembly, the Office of the Legislative Assembly, a person employed under the *Legislative Assembly (Members' Staff) Act 1989* (ACT) or an officer of the Assembly) or an entity prescribed by regulation.

What is a disclosable matter?

PRIVATE SECTOR whistleblower laws

Legislation	Disclosable matters
Corporations Act 2001 (Cth)	› Concerns fraud, negligence, default, breach of trust/duty or an improper state of affairs or circumstances relating to a company; › Constitutes an offence against a range of corporate and financial sector legislation specified under the *Corporations Act*; › Constitutes an offence against any law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more; › Represents a danger to the public or the financial system; or › Is otherwise prescribed by regulation. › Emergency disclosures relating to concerns about substantial and imminent dangers to the health or safety of one or more persons or to the natural environment.
Tax Administration Act 1953 (Cth)	› Information which indicates misconduct, or an improper state of affairs or circumstances, in relation to tax affairs (meaning affairs relating to any tax imposed by or under, or assessed or collected under, a law administered by the Commissioner). › Information which may assist the eligible recipient to perform duties or functions in relation to the tax affairs of the entity or an associate (within the meaning of section 318 of the *Income Tax Assessment Act 1936*) of the entity.
Fair Work (Registered Organisations) Act 2009 (Cth)	› Act or omission that contravenes, or may contravene, a provision of the Act, the *Fair Work Act 2009* (Cth) or the *Competition Consumer Act 2010* (Cth). For example, using a registered organisation's resources to favour one candidate over another in a registered organisation's election. › Act or omission that constitutes, or may constitute, an offence against a law of the Commonwealth.

What is a disclosable matter?

PUBLIC SECTOR whistleblower laws

Legislation	Disclosable Matters
Public Interest Disclosure Act 2013 (Cth)	› Conduct that contravenes a law of the Commonwealth, a State or a Territory, or conduct in a foreign country that contravenes a law in that country or is otherwise applicable to the agency, public official or contracted service provider and corresponds to a law in force in the Australian Capital Territory. › Conduct that perverts, or is engaged in for the purpose of perverting, or attempting to pervert, the course of justice or involves, or is engaged in for the purpose of, corruption of any other kind. › Conduct that constitutes maladministration, including conduct that is based, in whole or in part, on improper motives or is unreasonable, unjust or oppressive or is negligent. › Conduct that is an abuse of public trust. › Conduct that is fabrication, falsification, plagiarism, or deception, in relation to proposing scientific research, carrying out scientific research or reporting the results of scientific research; or misconduct relating to scientific analysis, scientific evaluation or the giving of scientific advice. › Conduct that results in the wastage of relevant money (within the meaning of the *Public Governance, Performance and Accountability Act 2013*), relevant property (within the meaning of that Act), money or property of a prescribed authority. › Conduct that unreasonably results in a danger to the environment or results in, or increases, a risk of danger to the environment. › Conduct of a kind prescribed by the PID rules. › Conduct engaged in by a public official that involves, or is engaged in for the purpose of, the public official abusing his or her position as a public official. › Conduct engaged in by a public official that could, if proved, give reasonable grounds for disciplinary action resulting in the termination of the official's engagement or appointment.
Public Interest Disclosures Act 2022 (NSW)	› Conduct that includes an allegation of, or otherwise shows or tends to show, serious wrongdoing* by an agency, public official associated with the agency or that otherwise affects, or might affect the exercise of the functions of the agency. *Under the *Public Interest Disclosures Act 2022* (NSW), serious wrongdoing means one or more of the following: corrupt conduct, a government information contravention, a local government pecuniary interest contravention, serious maladministration, a privacy contravention or a serious and substantial waste of public money.

Legislation	Disclosable Matters
Public Interest Disclosure Act 2018 (SA)	› Conduct that relates to an appropriate disclosure of environmental and health information*. › Conduct that relates to an appropriate disclosure of public administration information**. *Under the *Public Interest Disclosure Act 2018* (SA), environmental and health information means information that raises a potential issue of a substantial risk to the environment or to the health or safety of the public generally or a significant section of the public. **Under the *Public Interest Disclosure Act 2018* (SA), public administration information means information that raises a potential issue of corruption, misconduct or maladministration in public administration.
Public Interest Disclosures Act 2002 (Tas)	› Conduct that a public officer believes another public officer or a public body has engaged, is engaging or proposes to engage in improper conduct in their capacity as a public officer or public body or has taken, is taking or proposes to take detrimental action. › Conduct that a contractor who believes that the public body with which the contractor has entered into a contract has engaged, is engaging or proposes to engage in improper conduct in its capacity as a public body or has taken, is taking or proposes to take detrimental action.
Public Interest Disclosure Act 2010 (Qld)	› A substantial and specific danger to the health or safety of a person with a disability. › The commission of an offence against a provision, or condition imposed under a provision mentioned in schedule 2 of the Act, if the commission of the offence is or would be a substantial and specific danger to the environment. › The conduct of another person that could, if proved, be a reprisal.
Independent Commissioner Against Corruption Act 2017 (NT)	› Conduct engaged in by a public officer or by a public body that is improper conduct. *Under the *Independent Commissioner Against Corruption Act 2017* (NT), improper conduct includes corrupt conduct, misconduct, unsatisfactory conduct, anti-democratic conduct, conduct constituting an offence against the Act.

Legislation	Disclosable Matters
Public Interest Disclosures Act 2012 (Vic)	› Information that shows or tends to show, or that a person reasonably believes shows or tends to show, a person, public officer or public body has engaged, is engaging or proposes to engage in improper conduct*. › Information that shows or tends to show, or that a person reasonably believes shows or tends to show a public officer or public body has taken, is taking or proposes to take detrimental action** against a person. *Under the *Public Interest Disclosures Act 2012* (Vic), improper conduct means corrupt conduct, conduct of a public officer or public officer that is a criminal offence, serious professional misconduct, dishonest performance of public functions, an intentional or reckless breach of public trust, misuse of information or material acquired in the course of performance of the functions of the public officer or public body, a substantial mismanagement of public resources, a ssubstantial mismanagement of public resources, a substantial risk to the health or safety of one or more persons or a substantial risk to the environment; or conduct of any person that adversely affects the honest performance by a public officer or public body of their functions as a public officer or public body or is intended to adversely affect the effective performance or exercise by a public officer or public body of the functions or powers of the public officer or public body and results in the person, or an associate of the person, obtaining a licence, permit, approval, authority or other entitlement under any Act or subordinate instrument; or an appointment to a statutory office or as a member of the board of any public body under any Act or subordinate instrument; or a financial benefit or real or personal property; or any other direct or indirect monetary or proprietary gain that the person or associate would not have otherwise obtained; or conduct of any person that could constitute a conspiracy or attempt to engage in any such conduct. ** Under the *Public Interest Disclosures Act 2012* (Vic), detrimental action includes action causing injury, loss or damage, intimidation or harassment, discrimination, disadvantage or adverse treatment in relation to a person's employment, career, profession, trade or business, including the taking of disciplinary action.
Public Interest Disclosure Act 2003 (WA)	› Information that constitutes public interest information*. *Under the *Public Interest Disclosure Act 2003* (WA), public interest information means information that tends to show that, in relation to its performance of a public function, a public authority, a public officer, or a public sector contractor is, has been, or proposes to be, involved in improper conduct, an act or omission that constitutes an offence under a written law, a substantial unauthorised or irregular use of, or substantial mismanagement of, public resources or an act done or omission that involves a substantial and specific risk of an injury to public health, prejudice to public safety or harm to the environment or a matter of administration that can be investigated under section 14 of the *Parliamentary Commissioner Act 1971* (WA).
Public Interest Disclosure Act 2012 (ACT)	› Conduct including action or a policy, practice or procedure of a public sector entity, or public official for a public sector entity is maladministration. › Conduct including an action or a policy, practice or procedure of a public sector entity, or public official for a public sector entity that results in a substantial and specific danger to public health or safety, or the environment.

11. Personal Assessment Tool

This resource is derived from the legal section of The Signals Network's Tech Worker Handbook and is meant to help you make informed decisions, to give a balanced and concrete overview of the possibilities and pathways.

These are questions to consider when you are thinking about speaking out regarding wrongdoing at your company. Not all of them will apply in every case, and you shouldn't feel you need to answer positively to all of them before speaking out. These questions are helpful to assess where you are and what you are willing to go through in order to speak out.

MY OBJECTIVES

What do I hope to achieve by speaking out? **What are my intentions?** What impact do I want to have? **How realistic is it that I will make this impact?** What are the paths/leverages to achieving my goals?

What level of risk (professional, financial, legal, personal, etc.) am I willing to take to achieve my goals?

Would I be okay if the information I revealed didn't have the impact or achieve the objectives I wanted it to? "Sometimes whistleblowers' valid objective is to do the right thing so they can live with themselves, regardless of the impact." Tom Devine, Legal Director of the Government Accountability Project

What would I like my life to look like after speaking out? What would I like to see happen to be at peace with my decision so that I can move on?

Why is speaking out externally the best option over an alternative solution (i.e., internal reporting, speaking with colleagues, talking to the board, etc.)?

WHISTLEBLOWING PROCESS

Is this objectively misconduct? Am I in a position to know that what I see as misconduct really is a misconduct? **Does my job position provide sufficient insight to ensure my conclusions are not the mistaken product of tunnel vision, even if my information is accurate?**

Will knowledgeable peers and colleagues support my concerns, and help to expand the record from my personal knowledge?

Have I read other accounts of whistleblowers to understand what the process can be like?

Am I willing to commit to a multi-year endeavor (one year, three years, five years, or more) and what support will I need to do so?

Am I willing to invest significant amounts of time working with lawyers, educating NGOs, government investigators, Congress, and the media?

Do I understand how to engage properly with the media?

How do I feel about repeated public speaking engagements?

EMOTIONAL SUPPORT

Do I have an emotional support system? Who do I turn to for emotional support? (Partner, family, friends, religious mentor, professional mentor, therapist, etc.)

Are there other people at the company who would help me in this effort without getting me in trouble?

Do I have a plan for countering retaliation or negative things the company may say about me?

Can I remain sufficiently centered and detached to emotionally withstand inevitable smear campaigns?

Who are my allies and who are the people who would work against my effort?

Am I prepared for the potential trauma caused by whistleblowing?

Do I have a system of evaluating who I can trust with sensitive information?

Do I have pre-existing medical conditions that could be aggravated by stress?

LEGAL SUPPORT

Do I know where to find legal support for my case? What type of lawyer do I need to reach out to (i.e., employment lawyer, whistleblower lawyer, healthcare fraud lawyer, etc.)?

Do I have a secure way of reaching out? Personal phone/computer? Signal Messenger app? Protonmail?

Do I have a way to pay for a lawyer if they do not work fully on contingency?

Do I have a friend or a family member who is a lawyer? To advise me? **To find the right lawyer?** To help read my lawyer engagement letter, etc?

Have I prepared a concise summary of my case, and a timeline of key events to have ready for initial interviews with prospective lawyers?

EMPLOYMENT

Will I try to find another job before revealing the information?

What is my exit plan for my current role? Should I resign? What happens if I get fired? **What will happen to my immigration status (if applicable)?**

What other kinds of jobs would I like to have?

Would I be okay not working in this industry again?

Would I be okay not working in a similar role again?

FINANCES

Will I try to find another job before revealing the information?

What is my exit plan for my current role? Should I resign? What happens if I get fired? **What will happen to my immigration status (if applicable)?**

What other kinds of jobs would I like to have?

Would I be okay not working in this industry again?

Would I be okay not working in a similar role again?

CONSIDERATIONS ABOUT **STAYING ANONYMOUS**

Will an anonymous internal disclosure effect change? Or will it give the wrongdoers an opportunity to cover up the problem?

Does the anonymous channel, such as a hotline, operate with credible, effective technology to prevent exposure?

Will remaining anonymous sustain my access to ongoing evidence and developments that the institution is trying to conceal?

Can I prove my allegations with information/ documents that do not require my public explanation?

Can this information/documentation be traced back to me because only a small group of people have access to them or because my copies are uniquely marked? (Beware of trace-backs through printers' identifications or email trails.)

How likely is it that I will be the focus of suspicion because of my previous efforts to raise concerns?

Can I act nonchalantly when these documents are disclosed so as not to attract suspicion?

Do I feel comfortable and justified in being evasive or not telling the complete truth if confronted by my boss about the disclosure?

Am I prepared for the possibility that somehow my anonymity is broken without my consent?

CONSIDERATIONS ABOUT **GOING PUBLIC**

Are my family and I financially and mentally prepared for a protracted public fight with my employers and exposure to attacks to prove my allegations? And to try to retain a job?

Am I mentally ready to have my fellow workers and perhaps some friends turn against me because my public disclosures threaten the institution's health and their jobs?

Will going public cut off support from witnesses who would otherwise back my charges in official proceedings?

Will going public cut off the flow of evidence necessary to prove my charge or more effectively make a difference, and, if so, are the benefits from public solidarity more significant?

Am I ready for personal attacks against my character and to have any past indiscretions made public?

Do I have enough evidence to prove my charges without having to go back to my workplace?

Even if I can prove my initial allegations, would I be more valuable if I didn't go public and kept my access to new information?

Am I sure that my motivations are to expose the wrongdoing on behalf of the public interest and not just for revenge, a quest for financial gain, or public attention?

Am I financially and mentally ready to risk my career?

Am I ready to have the professional reputation of someone who attacked their employer?

12. Information Security

Digital Security Best Practices

Purpose

The purpose of this section is to serve as a guide to digital security best practices. It provides various strategies and tools to improve the security of both personal and professional digital communication and storage systems. This includes actionable steps, recommendations on technologies to use and avoid, guidelines on secure usage of email, Signal messaging, and Zoom, as well as advice on securing hardware such as desktops, laptops, and mobile devices. Additionally, it offers guidance on social media usage, personal safety precautions, and resources for further assistance.

Immediate actions

- **Delete unused or old social accounts:** To minimise your digital footprint and limit potential exposure of personal information, it's important to delete all unused or old social accounts. This includes removing all old posts, which might contain outdated or sensitive information.
- **No public personally identifiable information:** To protect your privacy, make sure you do not share any personally identifiable information publicly. This includes location details in any public post. Delete any posts that contain images of your home, family, or anything that can be used to identify you or your location.
- **Two-factor authentication for social accounts:** For all your social accounts, such as Twitter, LinkedIn, etc., it's crucial to have two-factor authentication enabled. This adds an extra layer of security to your accounts by requiring a second form of verification in addition to your password.
- **Two-factor authentication for personal online accounts:** For all your personal online accounts, like banking and email, two-factor authentication must be enabled immediately. This helps to prevent unauthorised access to your accounts by requiring a second form of verification alongside your regular login details.
- In addition to Two-Factor authentication, use a new additional secure login via Passkeys. This feature is supported by Google Workspace and many other platforms.

Tools & Services

Recommendation summary

1. Use Password Managers (and enable their two factor authentication capability): Tools include 1Password, LastPass.
2. Set Strong, Unique Passwords: For every online account.
3. Enable Multi-factor Authentication: Use apps like Authy, Google Authenticator.
4. Use a VPN: For secure and private browsing such as Mullvad.
5. Install Ad-blockers: To prevent unwanted ads and potential malware.
6. Regularly Update Your Software: Always use the latest versions.
7. Use Encrypted Messaging: Signal is highly recommended.
8. Use Secure Video Conferencing: Zoom with specific security settings.
9. Ensure Data Backups: iCloud, Google Cloud are recommended.

Discouraged and Encouraged Secure Tech

Due to known security and cross-platform compatibility issues, certain technologies should not be used for sensitive communications. Alternatives are provided for each technology.

Avoid using:

- SMS/text messages (use Signal instead)
- Slack (use Signal Groups instead, if possible)
- iMessage (use Signal instead, as it's insecure for SMS conversations)
- iCloud Drive (use Google Docs with two-factor protection instead)
- Office 365 (use Google Docs with two-factor protection instead)
- DropBox (use Google Drive with two-factor protection instead)
- Google Meet or Google Chat (use secured Zoom or Signal instead)

Security Rationale: To minimise potential points of failure, we aim to reduce the number of platforms used for critical functions. Messaging platforms lacking end-to-end encryption (SMS) or those that only work on an Apple platform (iOS) are discouraged. Additionally, we advise against using legacy applications from Google, such as Hangout Classic or Duo.

Below are *key recommended technology platforms*, along with *recommended security standards*

Email

Requirements

- All users must use two-factor authentication on their email accounts.
- Email accounts should be managed by a professionally managed IT solution. Google Workspace-based professional accounts are acceptable if professionally managed; personal Gmail accounts are not.
- All accounts must have a strong password/passphrase of 16 or more characters.
- Users must not use SMS as their second authentication factor, but may use an authentication app, such as Authy, Google Authenticator, 1Password Authenticator, or LastPass Authenticator.
- Google Hangout Classic and Google Duo should not be used, as they are deprecated products. Instead, secured Zoom or Google Meets in G Suite should be used.

Recommendations

- Users should not click on potential phishing links sent via email until they have verified the source and intent of the link through another medium, such as a phone call or Signal.
- Account logins and passwords should never be sent as plain text in an email. This is to protect against unauthorised access in case the email account is compromised.
- Recommend use of a hardware key as a second authentication factor. For Google accounts, we recommend a YubiKey or the Titan Security Key (UTF or Universal Two Factor) device as the second factor.
- If permitted by their IT provider, we recommend use of an account with Google's Advanced Protection.

Security Rationale

Email is one of the oldest technologies still used online and its security has improved over time. However, due to the need for backward compatibility with older email providers and the variety of email clients and providers, email cannot be fully trusted to be secure. While some email providers support end-to-end encryption, others do not. Many email clients do not visually indicate whether you are sending to an email address that supports this encryption option. Therefore, we recommend replacing email communications with Signal, which supports end-to-end encryption by default and uses a single client per platform when possible.

Signal

Requirements

- **Always use the latest version of Signal** for mobile and desktop, and updates should be installed as new releases are offered.
- **Deploy the "Use Registration Lock"** setting to prevent unwanted new devices from accessing your account.
- **Turn off iCloud call history sharing.** Signal allows you to look at your call history from your phone app. A useful feature, however, is that if the users have any cloud-based backup system to their phone and computer, they need to turn off this feature, and in Signal, choose "Show Calls in Recents" and have this Disabled.
- **Enable Signal's Screen Lock settings.**
- **Recommended: set "Disappearing Messages" to 1 week.** This gives enough time for chats and interaction, but after 1 week, it will automatically remove all posts from all users' phones.

Recommendations

- **Use Signal for communication as much as possible.**
- Signal Video and Audio calls can be used for particularly sensitive conversations to reduce the threat of "man in the middle" eavesdropping. This assumes that "Show Calls in Recents" is off, and the call metadata is secured to the application.
- Anyone who wishes to use Signal, but does not want their mobile phone number visible to others, **can use the 'username' function and set 'Who can find me by phone number' to 'Nobody'.**

Security Rationale

Signal has several security features that make it the best currently available option for secure communication, including but not limited to end-to-end encryption, a single client for each platform, and the option of automatically removing messages from the inbox after a certain amount of time.

Therefore, Signal should **be the primary messaging solution for all text-based IM and group communication.** We recommend using email or SMS messaging only when Signal messaging cannot work for logistical or technical reasons.

All outreach and communication should be done over Signal unless there is a technical reason why it cannot be.

Zoom

While Zoom has had several noted security issues during the pandemic, they have addressed those in rapid new release versions. Given its widespread use, Zoom remains a primary choice for organising and collaborating via video online but must be secured using the following requirements.

Requirements

- **Use the latest version of the Zoom client for** a computer or mobile phone and must continue to update to the latest new release versions.
- **Use a 16+ digit strong password or passphrase** when using the Zoom application and use their two-factor secured email address for login credentials.
- **Links to upcoming Zoom events should not be shared publicly or in emails.** Instead, they can be shared as part of secure calendar invites.
- **Use unique randomised passwords for Zoom meetings and meeting IDs for each meeting** and do not share them publicly.Meeting passwords should be set so they do not automatically embed inside the Zoom chat URL.
- All Zoom meetings should **not allow attendees to enter before the host.**
- All Zoom meetings **must have all participants authenticated** to join the meeting.
- Unless needed, all Zoom meetings **should turn off file sharing.**
- All Zoom meetings should **only allow the host or cohosts to screen share.**
- All Zoom meetings should be set NOT to allow recording of the meeting by participants, and the ability to autosave chats should be OFF.
- Recording a Zoom meeting also saves any chat messages, even private ones.

Recommendations

- Highly sensitive meetings can be locked after all participants have joined.
- Highly sensitive meetings can have a Waiting room where each authenticated user is added to the chat individually beforethe meeting begins.

Security Rationale

During the COVID-19 lockdowns, Zoom has become an essential and widespread business tool, and though they had some well-publicised security issues as they came into more widespread use, the bulk of those issues appear to be resolved. Zoom's scalability, ease of use, and cross-platform compatibility, particularly for calls with high numbers of participants and screen sharing, continue to make it the best currently available solution for SVF audio/videoconferencing and webinar needs. The security measures we recommend align with security experts' recommendations for ensuring that Zoom calls are secure.

Hardware & Devices

Desktops and Laptops

Recommendations

1. **Update Operating Systems Regularly:** Ensure that you are using the very latest operating system on your desktops and laptops, regardless of whether you use MacOS or Windows. Regularly update all patches and software updates.
2. **Update All Major Software Applications:** Ensure all major software applications, web browsers, PDF viewers, Office applications are updated to the most current and secure versions.
3. **Ensure HTTPS is set by Default:** All major browsers have native support for HTTPS-only mode. Confirm that *Always use Secure Connections* is enforced.
4. **Remove Adobe Flash:** Disable Adobe Flash completely or set it to "click to run" on your desktop or laptop web browser. This plugin is known for its security vulnerabilities.
5. **Set WIFI to Use WPA2 Password Encryption:** For both home and work WIFI, ensure that you are set to use the more secure WPA2 password encryption.
6. **Backup Data in Real Time:** Ensure your laptop, desktop, and network content is backed up in real time or near real time. iCloud, Google Cloud, or other similar platforms are highly recommended for personal devices.
7. **Full Disk Encryption:** Utilise full disk encryption on laptops either using BitLocker (Windows) or FileVault (Mac). Alternatively, use VeraCrypt on Windows devices.

Security Rationale

Desktops and laptops serve as critical points of vulnerability when they lack the most recent security patches and updates, including all essential software applications such as browsers, web plugins, Office Applications, and networks. Enhancing the security of these devices significantly involves regularly updating operating systems and software applications, employing encrypted connections, removing insecure plugins, using secure WIFI password encryption, and utilising real-time backup services.

Mobile Devices

Recommendations

1. **Use Recent Versions of Mobile Operating System:** We recommend all users use a recent version of their smartphone's operating system. For Apple iPhone users, ensure you have the most up-to-date iOS versions and continuously install new software updates as they occur. Android users should also ensure they are using the latest version of their Android OS.
2. **Secure Login and Password:** For Apple users, use complex passwords that meet our recommended standards for your Apple ID login and password. Also, use Two-Factor Authentication for your Apple ID. For Android users, ensure your Google account password is strong and enable Two-Factor Authentication.
3. **Manage Location Services:** For both iOS and Android users, change the settings so that only very critical applications (such as Maps applications) have access to your "location services." Even then, only set these applications to access location services when the applications are running.
4. **Encrypt Backups:** For iPhone users, ensure that iTunes and iCloud encrypt all data backups. Android users should use Google's backup service, which automatically encrypts backups.
5. **Limit Logins:** For both iPhone and Android users, preset your device to automatically wipe out all the data after a certain number of failed passcode attempts.

Security Rationale

In today's world, we increasingly work and live through our mobile devices, which carry key communications, emails, passwords, and other data. This makes them vulnerable to attacks, especially voice communication, internet chats, and call information. The Android system is somewhat less secure than the Apple iPhone platform, being more open to security breaches. Therefore, we strongly recommend a series of actions to enhance the security of your mobile devices. These include regularly updating operating systems, using encrypted connections, limiting login attempts, encrypting backups, and managing location services. By implementing these measures, we can significantly improve the security of our mobile devices.

Social Media

Recommendations

- Delete Old Posts: Remove any outdated or irrelevant posts from your social media platforms. This can help reduce the risk of unwanted information being used maliciously.
- Audit Your Own Accounts: Regularly review your social media accounts to ensure all information is accurate and up-to-date. This includes checking privacy settings, reviewing friend lists, and deleting any unnecessary information.
- Make Accounts Private: Adjust your social media settings so that only friends or approved followers can see your posts. This can greatly reduce the risk of unwanted individuals or entities accessing your information.
- Separate Work from Personal Accounts: Try to keep your professional and personal social media accounts separate. This can help protect your personal information from being exposed through your professional interactions.
- Remove Family Details and Information: To ensure the privacy and safety of your family members, avoid sharing sensitive details about them on social media. This includes their full names, locations, schools, or workplaces.
- Avoid Using Geotag Functions on Social Media Posts: Geotagging can reveal your exact location to anyone who views your post. To protect your privacy, it's best to avoid using this function.
- Avoid Posting Photos That Include Identifying Information: Try not to share pictures that include things like house numbers, car plates, or anything else that could be used to identify you or your location.
- Use Privacy Tools: Consider using online tools, like Block Party (https://www.blockpartyapp.com/privacy-party/), which can help you control what you see and who can interact with you on social media platforms. This can help reduce the risk of harassment or unwanted interactions.

Personal Safety

Recommendations

- Google Alerts on Who You Are: Set up Google Alerts for your name and other personal identifiers to monitor the internet for any new mentions or uses of your information.
- PimEye Yourself: Use the PimEye facial recognition search engine to see where images of your face may be posted online. This can help you identify any unauthorised or unwanted uses of your photos.
- Turn on Credit Freezes: Activate credit freezes with all major credit reporting agencies to prevent unauthorised individuals from learning detailed personal information about you or opening new accounts in your name.
- Have a Family “Code Word” to Verify Yourselves: Establish a code word or phrase with your family members that can be used to verify identity in communications, especially in situations that might involve impersonation or fraud.
- Transition Family to Signal: Encourage your family members to start using Signal, a highly secure messaging app, for all family communications to enhance privacy and security.
- Invest in a Privacy Service: Consider subscribing to a privacy service, which can provide additional protections such as encrypted email, virtual private networks (VPNs), and data breach alerts.
- Check on "Have I Been Pwned": Regularly enter your email addresses into the "Have I Been Pwned" website to check if your accounts have been compromised in any recent data breaches.

Checklist

Security Setup and Practices

- **Enable Two-Factor Authentication (2FA):** Verify if 2FA is enabled on all accounts, using tools like 1Password or LastPass.
- **Set Strong, Unique Passwords:** Check if all online accounts have strong, unique passwords.
- **Enable Multi-Factor Authentication (MFA):** Ensure MFA is activated wherever possible, using apps like Authy or Google Authenticator.
- **Use a VPN:** Confirm the use of a VPN for secure and private browsing.
- **Install Ad-Blockers:** Check for the installation of ad-blockers to prevent unwanted ads and potential malware.
- **Software Updates:** Ensure that all software is regularly updated to the latest versions.
- **Encrypted Messaging:** Verify the use of encrypted messaging apps like Signal.
- **Secure Video Conferencing:** Check if Zoom is being used with the recommended security settings.
- **Data Backups:** Ensure regular data backups are in place using services like iCloud or Google Cloud.

Technology Use: Discouraged and Encouraged

- **Avoid Certain Technologies:** Avoid certain discouraged technologies (e.g., SMS/text messages, Slack, iMessage, iCloud Drive, Office 365, DropBox, Google Meet/Chat) for sensitive communications.
- **Encouraged Technologies:** Ensure the use of recommended secure alternatives (e.g., Signal for messaging, Google Docs with two-factor protection, secured Zoom).

Email Security

- **Two-Factor Authentication for Email:** Verify that 2FA is enabled on all email accounts.
- **Professionally Managed IT for Email:** Ensure email accounts are managed by a professional IT solution, preferably Google Workspace-based accounts.

Social Media and Personal Information Security

- **Monitor Personal Information:** Check if Google Alerts are set up for personal identifiers to monitor the internet for new mentions.
- **Online Presence:** Use PimEye or similar services to check where images of faces are posted online.
- **Credit Freezes:** Confirm that credit freezes are activated with all major credit reporting agencies.
- **Family Security Practices:** Ensure a family “code word” is established, transition family communications to Signal, and consider investing in a privacy service.

General Security Measures

- **Regular Checks on "Have I Been Pwned":** Regularly check email addresses on "Have I Been Pwned" to see if accounts have been compromised in data breaches.

13. Endnotes

1 Popularised in Reid Hoffman and Chris Yeh's book, Blitzscaling: The Lightning-Fast Path To Building Massively Valuable Companies. The website describes the concept as: "Blitzscaling is a specific set of practices for igniting and managing dizzying growth; an accelerated path to the stage in a startup's life-cycle where the most value is created. It prioritizes speed over efficiency in an environment of uncertainty, and allows a company to go from "startup" to "scaleup" at a furious pace that captures the market."

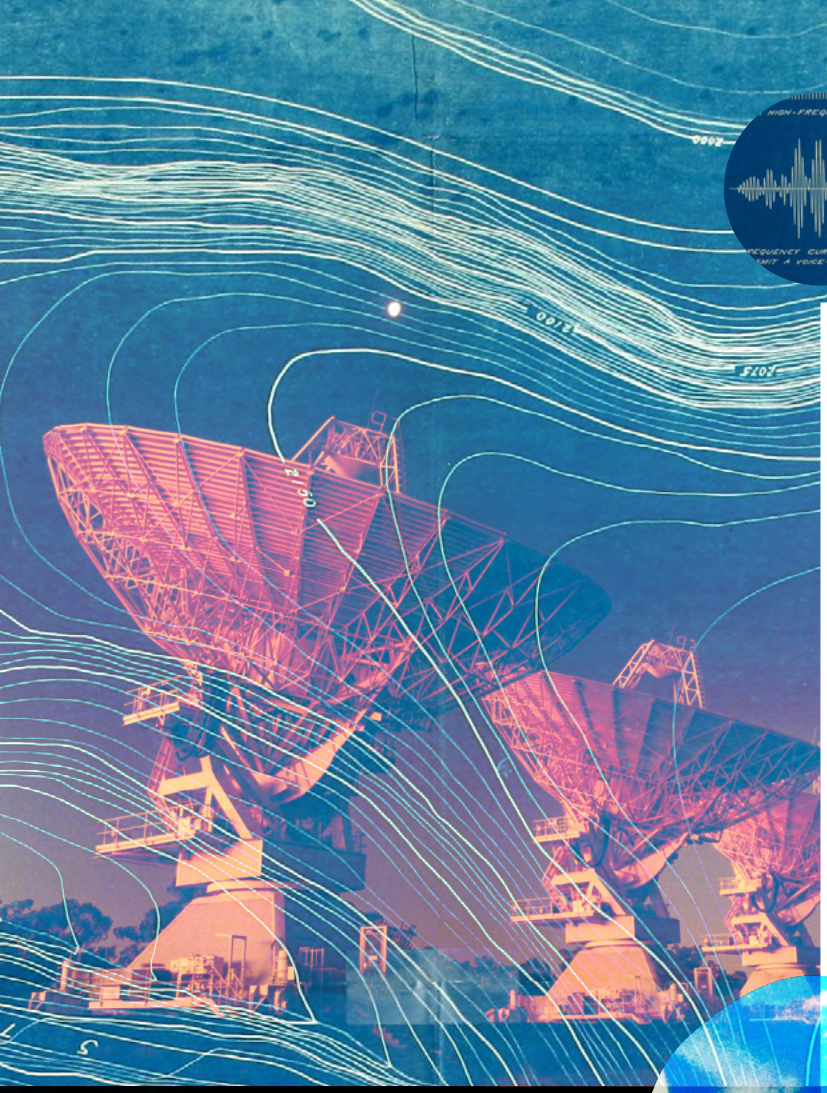
2 The concept originates from technical analyses of internet-based innovation, e.g. Barbara van Schewick's, Internet Architecture and Innovation (MIT Press, 2012), Kelsie Nabben and Michael Zargham, 'Permissionlessness' 2022 Internet Policy Review 11(1) https://doi.org/10.14763/2022.2.1656. The concept is occasionally used in critiques of the development and impact of technologies on society, see for example Maria Farrell and Robin Berjon's essay 'We Need To Rewild The Internet' Noema, 16th April 2024, https://www.noemamag.com/we-need-to-rewild-the-internet/, John Naughton 'The evolution of the Internet: from military experiment to General Purpose Technology' (2016) Journal of Cyber Policy 1(1) https://doi.org/10.1080/23738871.2016.1157619.

3 For an overview of A.I supply chains, see Ada Lovelace Institute, Allocating accountability in AI supply chains (2023) https://www.adalovelaceinstitute.org/resource/ai-supply-chains/

4 Human Rights Watch, Australia: Children's Personal Photos Misused to Power AI Tools 2nd July 2024, https://www.hrw.org/news/2024/07/03/australia-childrens-personal-photos-misused-power-ai-tools

5 Protections in the public sector are found in the *Public Interest Disclosure Act 2013* (Cth), *Public Interest Disclosures Act 2022* (NSW), *Public Interest Disclosures Act 2012* (Vic), *Public Interest Disclosure Act 2010* (Qld), *Public Interest Disclosure Act* 2018 (SA), *Public Interest Disclosure Act 2003* (WA), *Public Interest Disclosures Act 2002* (Tas), t*he Independent Commissioner Against Corruption Act 2017* (NT) and *the Public Interest Disclosure Act 2012* (ACT).

6 See Reset.Tech Australia (2023) Australians For Sale: Targeted Advertising, Data Brokering and Consumer Manipulation https://au.reset.tech/news/coming-soon-australians-for-sale-report/.



‘Whistleblowers make Australia a better place. They should be protected, not punished.’

If you have questions, please contact the Human Rights Law Centre’s Whistleblower Project.

https://www.hrlc.org.au/whistleblower-project