September 2024

UPDATE

Privacy Reform

On 12 September 2024 the P*rivacy and Other Legislation Amendment Bill 2024* was introduced in the House of Representatives. The Bill addresses 23 of the "agreed" proposals out of the 89 "agreed" and "agreed in principle" recommendations identified in the *Privacy Act Review Report* issued in February of 2023.

The changes that appear likely to require consideration and/or action by regulated entities are:

1. **Security:** The *Privacy Act 1987* (**Act**) will specify that security measures made in accordance with APP11 must include "technical and organisational measures". This change will take effect when the Act receives royal assent. Regulated entities may wish to implement and/or mention in their Privacy Policies "technical and organisational" measures to protect personal information if they do not already.
2. **Automated Decisions and Privacy Policies**: Where a regulated entity uses personal information to make a decision or "do a thing that is substantially and directly related to making a decision" which could "significantly affect the rights or interests of an individual", the following details must be included in its Privacy Policy:
   - "the kinds of personal information used in the operation of such computer programs; and
   - the kinds of such decisions made solely by the operation of such computer programs; and
   - the kinds of such decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs."

   This change will commence on a date fixed by proclamation or 6 months from Royal Assent. In response to this change. Regulated entities must establish whether PI is used within their organisation for automated decision making and adjust collection notices and privacy policies accordingly.

That Bill also makes the following changes:

1. **A minor amendment to the objects of the Act** to promote the protection of privacy and recognize the public interest in protecting privacy.
2. **APP Codes**: The Privacy Commissioner must develop APP codes if directed by the Minister.
3. **Ministerial power to make an Emergency Declaration to enable sharing of PI**: The Minister can issue a declaration that enabling the sharing of PI for permitted purposes related to the emergency including to identify or assist affected individuals, assist law enforcement or emergency response and coordinate management of the response.
4. **Children's privacy**: The Commissioner must develop a Children Online Privacy Code within 24 months of the changes becoming law. Thes code will outline the standards and obligations for handling children's personal information. The Minister has the authority to direct the Commissioner to develop a code. The Minister can specify the matters the code must address and the entities that must comply with it. Before finalizing a code, the Commissioner must make a draft publicly available and invite submissions . The Minister can direct the Commissioner to develop temporary code which can be in force for up to 12 months and are not subject to disallowance under the Legislation Act 2003.

5. **Overseas data flows**: The Act is amended to include criteria for prescribing that a foreign country or binding scheme is acceptable under APP 8.3. .
6. **Ministerial Declaration power to enable the sharing of PI where there is an Eligible Data Breach:** The Minister will be able to issue a Declaration to allow controlled sharing of subject PI in order to prevent or reduce the risk of harm arising from a misuse of personal information about one or more individuals subject to the breach.
7. **Applying civil penalties for serious Interferences with Privacy**: The amendments set out a list of factors to consider in order to assess whether an interference with privacy is serious and applies the penalties set out in s13G (introduced by the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*) to serious interferences of Privacy: up to $50m or 30% of adjusted turnover in the relevant period.
8. **New power to issue infringement notices:** for breach of listed APPs and/or a failure to provide information as required by a notice issued under s66, not to exceed 2000 penalty units (Currently $660,000). The Regulatory Powers Act 2014 sets the maximum penalty for bodies corporate at 10,000 penalty units (currently $3.3m)
9. **New Federal Court powers**: In proceedings under the Act, the Federal court is empowered to give orders requiring any reasonable act or course of conduct, directions to engage or not engage in any act or practice and or requiring the publication or communication of any statement. .
10. **Commissioner to conduct public Inquiries**: The Commissioner is given power to conduct public inquiries relating to specified matter/s relating to privacy, including calling for submissions, examining witnesses and publishing reports.
11. **Additional possible determinations following Investigations**: The Commissioner is given power to determine after an investigation that the respondent perform any reasonable act or course of conduct to "… prevent or reduce any reasonably foreseeable loss or damage that is likely to be suffered". The Commissioner is given power not to decide a compliant already dealt with by an external compliant resolution scheme.
12. **New monitoring and investigation powers.** The Commissioner is given power to monitor operations of the privacy provisions of the Consumer Data Right rules in the *Competition and Consumer Act 2010*, Commonwealth and State authority obligations in relation to Pardons for persons wrongly convicted, and quashed convictions and spent convictions under the *Crimes Act 1914*, and under the *Data matching (Assistance and Tax) Act 1990* and the N*ational Health Act 1953*. Investigation powers are given in relation to those Acts, the *Digital ID Act 2024*, the *Healthcare Identifiers Act 2010* and the *My Health Records Act 2012*.
13. **Right of action for serious invasions of privacy**: A new cause of action for serious invasion of privacy is created. The cause of action arises where a person is subject to "intrusion on seclusion" and/or misuse of information relating to a person where the person "would have had a reasonable expectation of privacy" in the circumstances and the invasion was intentional or reckless and serious. Defences include that the subject action was in the public interest, required or authorised under law, necessary to prevent or lessen a serous threat to life, health or safety, or incidental to a proportionate, necessary and reasonable exercise of a legal right. National security agencies and Journalists acting in a professional capacity and subject to a code of practice are exempt.

The Criminal Code Act 1995 is amended by the insertion of two new offences of Doxxing:

- **A person must not use** a carriage service to make available, publish or otherwise personal data of one or more individuals in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those individuals. Penalty 6 years imprisonment.
- **A person must not use** a carriage service to make available, publish or otherwise personal data of one or more members of certain groups in a way that reasonable persons would regard as

being, in all the circumstances, menacing or harassing towards those individuals. The offence requires the individual making the publication to engage in the conduct due to a belief that the group is distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin. Penalty 7 years imprisonment.

For the purposes of these offences "personal data" means information about the individual that enables the individual to be identified, contacted or located.

By operation of S4B of the *Crimes Act 1914* the prison terms specified represent maximum financial penalties of 18,000 and 21,000 penalty units respectively. (currently $5,940,000 and $6,930,000)

Notably, the amendments **do not** include "agreed" or "agreed in principle" changes to privacy law related to changing the definition of PI to refer to information that "relates to" rather than being "about" and individual, expressly including inferred information in the definition of PI, the regulation of small business, coverage of employee records, the introduction of a processor/controller distinction, to Commissioner issued privacy standards for Journalists, facilitating the collection of PI for research, a raft of burdensome PI administrative requirements nor the new data subject rights of explanation, assistance and data erasure.

Combating misinformation and disinformation

The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* was also introduced to the House on 12 September 2024. The Bill gives Australian Communications and Media Authority (**ACMA**) powers to oversee and regulate digital platform services. The new law attempts to create framework to address misinformation and disinformation communicated using the services.

Obligations that will be imposed by the Bill include:

1. **Risk Management**: Digital platforms must assess and publicly report on risks related to misinformation and disinformation and implement risk management plans.
2. **Published Policie**s: Platforms must publish policies regarding misinformation and disinformation, as well as media literacy plans to help users identify misleading content.
3. **Complaints**: Platforms are required to establish processes for managing complaints about misinformation.
4. **Misinformation Code**s: Industry bodies may develop codes to prevent or respond to misinformation. The Codes must be approved by the Australian Communications and Media Authority (ACMA). Where no code exists or is deemed inadequate, ACMA may establish enforceable standards.
5. **Enforcement:** ACMA has the authority to enforce compliance, including issuing directions, requiring reports, and imposing civil penalties for non-compliance.

Key Concepts and Terms:

- **Digital Communications Platform**: Any service that enables interaction or sharing of content online including social media services and search engines.
- **Excluded dissemination** (i.e. dissemination not regulated) means the dissemination of parody or satire, professional news content, and reasonable dissemination for academic, artistic, scientific, or religious purposes. Professional news content is defined as content published in various formats (such as newspapers, TV, or websites) by individuals or organizations that follow recognized editorial standards and maintain editorial independence. News content is confined to content that reports, investigates or explains issues that engage public debate, inform democratic decision-making, or address significant current events.
- **Inauthentic behaviour** refers to the dissemination of content that is likely to mislead users, either through the use of automated systems or coordinated actions. It also includes efforts to evade enforcement of laws or platform terms, such as by disguising the identity, purpose, or

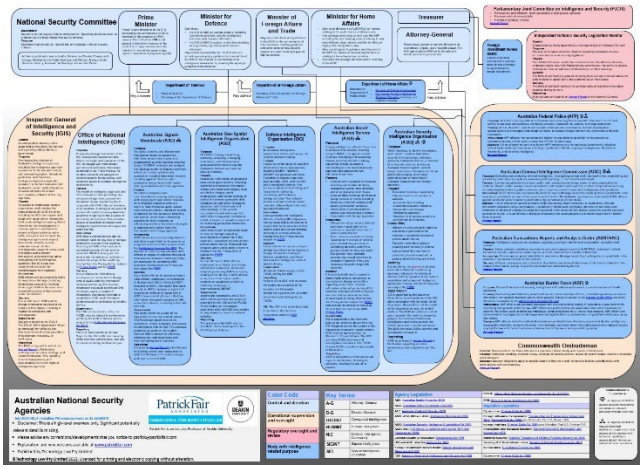
source of the content, inflating its popularity, or hiding the motives of those spreading it. Accordingly, this term appears to cover a range of technologies and methodologies used to manipulate social media platforms including Bots, Sock puppets, Astroturfing, Click Fairs, Amplification Algorithms, Hashtag manipulation, Echo Chambers and Filter Bubbles.

- **Misinformation**: means information that is "reasonably verifiable as false, misleading or deceptive, is reasonably likely to cause or contribute to serious harm and is not disseminated by excluded dissemination.
- **Disinformation:** has the same meaning as misinformation except that there are also grounds to suspect that the person disseminating, or causing the dissemination of, the content intends that the content deceive another person or the dissemination involves inauthentic behaviour.
- **Media Literacy Plan** A plan outlining how platforms will educate users to better identify misinformation.

Updated Chart of Australian National Security Agencies available for download

On 28 July 2024 the Prime Minister announced that responsibility for ASIO was being moved from the Home Affairs portfolio to the Attorney-General. Accordingly, the PFA Chart of National Security Agencies needed updating.

An updated version of the PFA chart of National Security Agencies is available for download here.



Please contact me if you have any questions regarding the matters discussed in this update. patrick@patrickfair.com 0411361534

You can subscribe to updates like this one at www.patrickfair.com